Table of Contents

Part I Welcome

1 About ........................................................................................................... 11
2 EventSentry Light ....................................................................................... 11

Part II Installing EventSentry

1 Requirements............................................................................................... 14
   Hardware Specifications for Sensors .............................................................. 18
   Databases ........................................................................................................ 18
2 Getting EventSentry ...................................................................................... 19
3 Licensing EventSentry ................................................................................ 21
   Entering a License .......................................................................................... 22
4 Local Installation (with installer, default) ................................................... 26
5 Updating to a new version .......................................................................... 27
   Updating to v5.0 ............................................................................................. 27
   Updating to v4.2 ............................................................................................. 29
   Updating to v4.1 ............................................................................................. 30
   Updating to v4.0 ............................................................................................. 31
   Updating to v3.5 ............................................................................................. 31
   Updating to v3.4 ............................................................................................. 32
   Updating to v3.3 ............................................................................................. 32
   Updating to v3.2 ............................................................................................. 33
   Updating to v3.1 ............................................................................................. 33
   Updating to v3.0 ............................................................................................. 33
   Updating from v2.7x to v2.90 ........................................................................ 35
   Updating from v2.60 to v2.70 ....................................................................... 35
   Updating from v2.50 to v2.60 ....................................................................... 36
   Upgrading from EventSentry Light ............................................................... 38
   Upgrading from the EventSentry Trial Version ........................................... 38
   Advanced Users ............................................................................................. 39
      Manually updating the Service ................................................................... 39
      Manually updating the GUI and documentation ....................................... 40
6 Moving EventSentry to a new server ......................................................... 40
7 Remote Agent Installation .......................................................................... 41
   Deploying the EventSentry Agent MSI ........................................................ 42
8 Web Reports ................................................................................................ 43

Part III Management Console / Utilities

1 Customizing ................................................................................................. 45
   General .......................................................................................................... 46
   Version Check / Welcome .......................................................................... 49
   Customizations ............................................................................................. 51
   Remote Update ............................................................................................. 51
   Features ........................................................................................................ 55
   Web Reports & Proxy .................................................................................... 55
   QuickTools .................................................................................................... 56
Part IV Working with EventSentry

1 Welcome Screen ........................................................................................................... 84

2 Event Log Viewer ......................................................................................................... 58
   Viewing Remote Event Logs ......................................................................................... 65
   Viewing Event Log Backup (.evt) Files ........................................................................ 65

3 Utilities .......................................................................................................................... 66
   Agent Database Status Utility ..................................................................................... 66
   Configuration Assistant .............................................................................................. 67
   Database Purge Utility ................................................................................................. 68
   Log Import Utility ....................................................................................................... 70
   Event Message Browser .............................................................................................. 72
   Protocol Parser (Collector) ........................................................................................ 73
   Remote Update Utility ................................................................................................. 74

4 Exporting, Importing and Saving the Configuration ..................................................... 74

5 Checking for New Versions ......................................................................................... 75

6 Testing Event Log Filter Rules .................................................................................... 76

7 Wizards .......................................................................................................................... 79

8 Toolbar (Legacy) .......................................................................................................... 80

9 Searching ...................................................................................................................... 81
   Searching for Filters ................................................................................................... 82

Part IV Working with EventSentry

1 Welcome Screen ........................................................................................................... 84

2 Collector .......................................................................................................................... 85
   Configuration ............................................................................................................... 86
   Security ....................................................................................................................... 89
   Multiple Collectors .................................................................................................... 91

3 Packages ........................................................................................................................ 92
   Package Options ......................................................................................................... 93
   Assigning Packages ................................................................................................. 95
   Setting Packages as Global....................................................................................... 96
   Assigning to Groups ................................................................................................. 97
   Assigning to Computers ............................................................................................ 98
   Blocking Package Inheritance ................................................................................ 100
   Downloading Packages ........................................................................................... 101
   (Un)Hiding Packages ............................................................................................... 104

4 Actions ........................................................................................................................... 105
   Managing Actions ...................................................................................................... 106
   Schedule .................................................................................................................... 108
   Action Options .......................................................................................................... 109
   Thresholds ................................................................................................................ 110
   Frequency ................................................................................................................ 112
   Action Activity .......................................................................................................... 112
   Dynamic Content Enhancement .............................................................................. 113
   Email (SMTP) .......................................................................................................... 113
   Troubleshooting Email (SMTP) .............................................................................. 118
   Display & Delivery Options ..................................................................................... 118
   Database .................................................................................................................... 121
   Setting up the database ........................................................................................... 124
   Database Schema ..................................................................................................... 124
   Event Log Consolidation .......................................................................................... 125

© <2002 - 2022> ... NETIKUS.NET ltd
Log File Monitoring ................................................................. 126
    Non-Delimited Log Files .................................................. 126
    Delimited Log Files .......................................................... 127
Service Monitoring ................................................................. 128
    Service Status ................................................................. 128
    Service History ............................................................... 129
Heartbeat Monitoring ............................................................. 130
    Heartbeat Status .............................................................. 130
    Heartbeat History ........................................................... 131
    Heartbeat Response Times ................................................. 131
Nessus .................................................................................. 132
Syslog .................................................................................. 132
Snmp .................................................................................. 133
Environment Monitoring ........................................................ 134
Compliance Tracking .............................................................. 135
    Process Tracking ............................................................ 135
    Logon Tracking ............................................................... 136
    Console Logons .............................................................. 136
    Network Logons .............................................................. 137
    Logon Failure Analysis .................................................... 137
    Domain Account Authentication ....................................... 138
User Logon By Server Type ..................................................... 139
Print Tracking ...................................................................... 140
File Access Tracking .............................................................. 141
    Account Management ..................................................... 142
    User Accounts ............................................................... 142
    Group Accounts ............................................................ 143
    Computer Accounts ........................................................ 144
    Policy Change Tracking ................................................... 145
Inventory ............................................................................. 146
    Software Monitoring ....................................................... 146
    Install Software ............................................................. 146
    Software History ............................................................ 147
    Uptime Monitoring .......................................................... 148
    Hardware Inventory ......................................................... 149
File Monitoring .................................................................... 150
    Performance Monitoring .................................................. 151
    Disk Space Monitoring .................................................... 152
Steps to Event Log Consolidation .......................................... 152
Troubleshooting Databases ................................................... 153
Web Reports ........................................................................ 153
Process .............................................................................. 155
    Options ......................................................................... 156
    Troubleshooting Processes ................................................ 157
    Event Log ....................................................................... 157
Syslog ................................................................................. 157
    Troubleshooting Syslog .................................................... 159
SNMP .................................................................................. 159
    Troubleshooting SNMP ................................................... 160
Pager (SNPP) ....................................................................... 161
    Troubleshooting SNPP ...................................................... 162
Service & Process Control ..................................................... 162
    Troubleshooting Service Control ....................................... 163
File ..................................................................................... 163
Content Filter .......................................................................................................................... 234
Advanced ............................................................................................................................. 237
Advanced Text Processing .................................................................................................. 239
Filter Processing .................................................................................................................. 240
Folders .................................................................................................................................. 242
Editing Filters ....................................................................................................................... 243
Thresholds ............................................................................................................................ 244
  Event Logs ........................................................................................................................... 249
Timers .................................................................................................................................... 253
Advanced Hour / Day Settings .............................................................................................. 256
  Day & Hour Configuration ................................................................................................. 257
  Expiration ........................................................................................................................... 259
  Boot Behavior ..................................................................................................................... 259
  Summary Notifications ...................................................................................................... 260
  Recurring Event Filters ...................................................................................................... 262
Monitoring Custom Event Logs ............................................................................................. 263
  Managing Custom Event Logs ........................................................................................... 264
  Monitoring Custom Event Logs .......................................................................................... 266
4 Log File Monitoring ............................................................................................................. 267
Creating File Definitions ........................................................................................................ 269
Defining Monitored Files ........................................................................................................ 274
Adding Files to a Log File Package ......................................................................................... 275
Consolidation & Monitoring Options ....................................................................................... 276
  Event Logs ........................................................................................................................... 277
5 System Health Monitoring ................................................................................................... 278
Alerts ...................................................................................................................................... 279
Service Monitoring ................................................................................................................ 280
  Advanced Options ............................................................................................................... 283
  Linux / Unix Configuration ................................................................................................. 284
  Event Log ............................................................................................................................ 285
Application Scheduler ........................................................................................................... 289
  Example Scripts .................................................................................................................... 292
  Event Log ............................................................................................................................ 294
Backup Event Logs .................................................................................................................. 295
  Detecting Full Event Logs .................................................................................................... 297
  Event Log ............................................................................................................................ 297
Process Monitoring ................................................................................................................ 298
  Event Log ............................................................................................................................ 300
Disk Space Monitoring .......................................................................................................... 301
  Override ............................................................................................................................... 303
  Event Log ............................................................................................................................ 304
Directory Monitoring ............................................................................................................. 306
  Event Log ............................................................................................................................ 308
Software / Hardware Inventory ............................................................................................... 309
  Event Log ............................................................................................................................ 316
Performance Monitoring ......................................................................................................... 320
  Counter Configuration ......................................................................................................... 322
    Windows Counters ............................................................................................................ 323
    SNMP Counters ................................................................................................................. 325
    Executables ......................................................................................................................... 328
  Alerts ................................................................................................................................... 329
  History & Trending ............................................................................................................... 334
  Event Log ............................................................................................................................ 335
<table>
<thead>
<tr>
<th>EventLog &amp; Database</th>
<th>341</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Directories</td>
<td>344</td>
</tr>
<tr>
<td>Event Log</td>
<td>346</td>
</tr>
<tr>
<td>NTP Monitoring</td>
<td>347</td>
</tr>
<tr>
<td>Event Log</td>
<td>348</td>
</tr>
<tr>
<td>Scheduled Tasks</td>
<td>349</td>
</tr>
<tr>
<td>Event Log</td>
<td>350</td>
</tr>
<tr>
<td>System Status Tray Application</td>
<td>352</td>
</tr>
<tr>
<td>Configuration</td>
<td>355</td>
</tr>
<tr>
<td>6 Security &amp; Compliance</td>
<td>356</td>
</tr>
<tr>
<td>Package Options</td>
<td>357</td>
</tr>
<tr>
<td>Requirements</td>
<td>357</td>
</tr>
<tr>
<td>Process Tracking</td>
<td>359</td>
</tr>
<tr>
<td>Sysmon Integration</td>
<td>361</td>
</tr>
<tr>
<td>Logon Tracking</td>
<td>363</td>
</tr>
<tr>
<td>Console Logons</td>
<td>364</td>
</tr>
<tr>
<td>Logon Activity</td>
<td>365</td>
</tr>
<tr>
<td>Print Tracking</td>
<td>367</td>
</tr>
<tr>
<td>Requirements</td>
<td>369</td>
</tr>
<tr>
<td>File Access Tracking</td>
<td>370</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>371</td>
</tr>
<tr>
<td>Setting up File Access Tracking</td>
<td>372</td>
</tr>
<tr>
<td>Access Masks &amp; Filter</td>
<td>374</td>
</tr>
<tr>
<td>Account Management Tracking</td>
<td>375</td>
</tr>
<tr>
<td>Audit Policy Monitoring</td>
<td>376</td>
</tr>
<tr>
<td>Registry Change Tracking</td>
<td>377</td>
</tr>
<tr>
<td>7 Validation Scripts</td>
<td>379</td>
</tr>
<tr>
<td>8 Environment Monitoring</td>
<td>381</td>
</tr>
<tr>
<td>Temperature / Humidity</td>
<td>383</td>
</tr>
<tr>
<td>Motion Monitoring</td>
<td>385</td>
</tr>
<tr>
<td>Smoke / Water</td>
<td>386</td>
</tr>
<tr>
<td>Event Logs</td>
<td>387</td>
</tr>
<tr>
<td>9 Heartbeat Monitoring</td>
<td>388</td>
</tr>
<tr>
<td>SNMP / SSH Monitoring</td>
<td>388</td>
</tr>
<tr>
<td>Adding Computers</td>
<td>390</td>
</tr>
<tr>
<td>Global Options</td>
<td>390</td>
</tr>
<tr>
<td>Group Options</td>
<td>392</td>
</tr>
<tr>
<td>Customizing Heartbeat Settings</td>
<td>395</td>
</tr>
<tr>
<td>Defining a Host as a Router</td>
<td>397</td>
</tr>
<tr>
<td>Setting Maintenance Schedules</td>
<td>398</td>
</tr>
<tr>
<td>Event Log</td>
<td>400</td>
</tr>
<tr>
<td>10 Network Services</td>
<td>402</td>
</tr>
<tr>
<td>Syslog Daemon</td>
<td>404</td>
</tr>
<tr>
<td>Database Consolidation</td>
<td>405</td>
</tr>
<tr>
<td>Syslog to Event Log</td>
<td>406</td>
</tr>
<tr>
<td>Unix/Linux Configuration</td>
<td>408</td>
</tr>
<tr>
<td>Snmp Trap Daemon</td>
<td>408</td>
</tr>
<tr>
<td>Mibs, Communities &amp; Users</td>
<td>409</td>
</tr>
<tr>
<td>Database Consolidation</td>
<td>411</td>
</tr>
<tr>
<td>Traps to Event Log</td>
<td>412</td>
</tr>
<tr>
<td>ARP Daemon</td>
<td>413</td>
</tr>
<tr>
<td>Event Log &amp; Database</td>
<td>414</td>
</tr>
</tbody>
</table>
Part VI Web Reports

1 Pages ........................................................................................................................................ 434
   Dashboard Pages .................................................................................................................. 435
   Tile Types ............................................................................................................................ 437
   Network Status .................................................................................................................... 440
   Health Matrix ...................................................................................................................... 441

2 Page Features ..................................................................................................................... 451

3 Reports & Jobs .................................................................................................................... 452
   Jobs ...................................................................................................................................... 453

4 Maintenance ....................................................................................................................... 455
   Maintenance Wizard ............................................................................................................ 455
   Collector Status .................................................................................................................... 456

5 Settings .................................................................................................................................. 457
   Profiles .................................................................................................................................. 457
   Access Control .................................................................................................................... 458
     Permissions & Privileges .................................................................................................. 459
   Preferences ........................................................................................................................... 460

Part VII Additional Tips and Resources ..................................................................................... 461

1 Database Tips ........................................................................................................................ 461
   Tuning the EventSentry Database ...................................................................................... 461
   Purging Records .................................................................................................................. 463
     Purging Records Automatically ...................................................................................... 466
   Archiving event log records .............................................................................................. 466
   Microsoft SQL Server ........................................................................................................ 468
     Encrypting Network Traffic with MSSQL ...................................................................... 468

2 Screenshots ........................................................................................................................... 473
   Main Configuration Window .............................................................................................. 473

© <2002 - 2022> ... NETIKUS.NET ltd
### Part VIII  Support, FAQ, Version History

1. Troubleshooting and FAQ ................................................. 571
2. Questions or Problems? .................................................. 571
   EventSentry Support ....................................................... 0
3. Version History ............................................................ 572
   Version Numbering System ............................................. 590
Part IX  Suggestions and Future Features

Part X  Credits

1 PostgreSQL .............................................................................................................. 592
2 PostgreSQL ODBC .................................................................................................. 592
3 Qt ........................................................................................................................... 593
4 GeoIP ...................................................................................................................... 601
5 cgminer .................................................................................................................. 601
6 RapidJSON ............................................................................................................. 602
7 Google Protocol Buffers ......................................................................................... 604
8 PCRE ....................................................................................................................... 604
9 Zlib ........................................................................................................................ 606
10 Boost ..................................................................................................................... 607
11 Crypto++ ............................................................................................................... 607
12 WinPCAP ................................................................................................................ 608
13 Tomcat, Play! Framework ...................................................................................... 611
14 jQuery ................................................................................................................... 615
15 OpenJDK JRE ...................................................................................................... 615

Index 0
1 Welcome

Full-spectrum, monitoring & compliance solution for servers and workstations.

This is the official documentation for EventSentry, the comprehensive resource that describes all features of EventSentry. Please note that all topics are directly linked from the Management Console and can be accessed by clicking the Help button throughout the management console.

Other resources are also available for first-time users that might be more helpful for getting started with the product:

- Web-Based Tutorials
- Screen Casts
- EventSentry Overview
- Best Practices

Other Formats
This manual is also available in the following formats at http://www.eventsentry.com/support/documentation:

- Online (HTML)
- Microsoft Help Format (.chm)
- iPad / iBook

Support
Answers to most questions can be found in the various areas on the product web site http://www.eventsentry.com, including the knowledge base and forums. If you have a question or problem with EventSentry, please try to find an answer through the following resources:

- Search all available resources online at http://www.eventsentry.com
- Search the Knowledge Base at http://www.eventsentry.com/support/kb
- Search the Forums at http://forums.netikus.net/

Email and telephone support is also available to registered and evaluation users. Please see below for a list of support options:

- Fill out our web form
- Send an email to support@netikus.net
Welcome

Thank you for using EventSentry!

Your NETIKUS.NET team.

1.1 About

EventSentry, developed by NETIKUS.NET ltd, is a WinXP - Windows 2003 - Windows Vista - Windows 2008 (R2) - Windows 7/8 - Windows 2012 (R2) - Windows 2019 application suite that actively monitors your server's (or workstation's) event log, system health and network devices.

Configure EventSentry to notify you if important events matching your filter criteria occur or consolidate your event logs into one central location such as a central ODBC database. You can be actively notified in several ways including Email, ASCII file, database, Unix Syslog, SNMP, HTTP, network message, process, and more. You can also monitor services, disk space, performance, processes and more. The Heartbeat monitor checks whether servers and network devices are up and running.

EventSentry also includes a Unix/Linux Syslog/SNMP server, which logs incoming Syslog packets and SNMP traps either to the Windows event log or a database. An optional NetFlow component visualizes NetFlow or sFlow data.

If you have purchased EventSentry - Congratulations! You have obtained a software product that comes with excellent support and a team that is devoted to making log, system and network monitoring as powerful as possible, while at the same time keeping our product as simple to use as possible. Any problem you have with EventSentry or monitoring will become our problem and we make every effort to resolve all issues as fast as possible.

This manual is also available in the following formats from https://www.eventsentry.com/support/documentation (you may click on the text to download or browse the alternate file immediately):

Online (HTML)
Microsoft Help Format (.chm)
Multimedia Help (.exe)

1.2 EventSentry Light

EventSentry Light is the freeware version of EventSentry and the successor to EventwatchNT that allows you to evaluate EventSentry for unlimited time. EventSentry Light offers only a few of EventSentry's features. We cannot offer support services for EventSentry Light; please purchase EventSentry for first-class support.

In a nutshell, EventSentry Light has the following limitations:

- No database and web reporting support is included
- No Security & Compliance features (Process, Logon, Account Management, ...) are available
- Support only available through our forums (https://helpdesk.eventsentry.com)

© <2002 - 2022> ... NETIKUS.NET ltd
Please see below for a **detailed feature comparison** between EventSentry and EventSentry Light:

<table>
<thead>
<tr>
<th>Feature Description</th>
<th>included in EventSentry Light</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actions</strong></td>
<td></td>
</tr>
<tr>
<td>SMTP Notification</td>
<td>yes</td>
</tr>
<tr>
<td>Syslog Notification</td>
<td>yes</td>
</tr>
<tr>
<td>SNMP Notification</td>
<td>yes</td>
</tr>
<tr>
<td>SNPP Notification</td>
<td>yes</td>
</tr>
<tr>
<td>Text File Notification (Plain Text, (X)HTML, CSV)</td>
<td>yes</td>
</tr>
<tr>
<td>Database Consolidation</td>
<td><strong>no</strong></td>
</tr>
<tr>
<td>Parallel Printer Notification</td>
<td>yes</td>
</tr>
<tr>
<td>Network Notification (aka &quot;net send&quot;)</td>
<td>yes</td>
</tr>
<tr>
<td>Process Notification</td>
<td>yes</td>
</tr>
<tr>
<td>Sound Notification, Desktop Notification</td>
<td>yes</td>
</tr>
<tr>
<td>Jabber Notification</td>
<td>yes</td>
</tr>
<tr>
<td>Shutdown Notification, Service Control Notification</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP Notification</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Filter (Event Log Monitoring) Options</strong></td>
<td></td>
</tr>
<tr>
<td>Event Log Packages</td>
<td>yes</td>
</tr>
<tr>
<td>Event Log Filters</td>
<td>yes</td>
</tr>
<tr>
<td>Filter Thresholds</td>
<td>yes</td>
</tr>
<tr>
<td>Filter Timers</td>
<td>yes</td>
</tr>
<tr>
<td>Monitor custom event logs</td>
<td>yes</td>
</tr>
<tr>
<td>Filtering based on Event log, severity, ID, source, category and text</td>
<td>yes</td>
</tr>
<tr>
<td>Filtering based on weekday and time of day</td>
<td>yes</td>
</tr>
<tr>
<td>Recurring Events</td>
<td>yes</td>
</tr>
<tr>
<td>Configure summary notifications</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Network Services</strong></td>
<td></td>
</tr>
<tr>
<td>Syslog Daemon</td>
<td>yes, no database logging</td>
</tr>
<tr>
<td>SNMP Trap Daemon</td>
<td>yes, no database logging</td>
</tr>
<tr>
<td>ARP Daemon</td>
<td>yes, no database logging</td>
</tr>
<tr>
<td><strong>Log File Monitoring</strong></td>
<td></td>
</tr>
<tr>
<td>Monitor non-delimited text files</td>
<td>yes</td>
</tr>
<tr>
<td>Monitor delimited text files</td>
<td>no</td>
</tr>
<tr>
<td>Consolidate text files to database</td>
<td>no</td>
</tr>
<tr>
<td><strong>System Health Features</strong></td>
<td></td>
</tr>
<tr>
<td>System Health Packages</td>
<td>yes</td>
</tr>
<tr>
<td>Service and Driver Monitoring</td>
<td>yes</td>
</tr>
<tr>
<td>Application Scheduler</td>
<td>yes</td>
</tr>
<tr>
<td>Event Log Backup / Clear</td>
<td>yes</td>
</tr>
<tr>
<td>Full event log detection</td>
<td>yes</td>
</tr>
<tr>
<td>Process Memory Monitoring</td>
<td>yes</td>
</tr>
<tr>
<td>Disk Space Monitoring</td>
<td>yes</td>
</tr>
</tbody>
</table>
Welcome

Directory Size Monitoring: yes
Software/Hardware Inventory: yes, but no hardware inventory or uptime collection
Performance Monitoring: yes, but no history reports
File Change Monitoring: yes
NTP Monitoring: yes

Included Utilities
Remote Update Utility: no
EventSentry Database Import Utility: no

Security & Compliance Features
Process Tracking: no
Logon Tracking: no
Print Tracking: no
File Access Tracking: no
Account Management Tracking: no
Policy Change Tracking: no

General Features
Groups: yes, max. 2
Process messages that occur during a server/workstation boot (Boot Scan): yes
Resend messages if SMTP/ODBC/Syslog server is unavailable: yes, only SMTP
Remote service administration: no
Remote Update: (Un)Install, update, configure, control remote installations: yes, up to two computers
Import & Link to Active Directory feature for remote update: no
Receive Syslog messages from remote Unix/Linux computers: yes, no database logging
Receive SNMP traps: yes, no database logging
View remote event logs in management application: yes
Import / Export configuration feature: yes
Custom Variable Support: yes
Heartbeat Monitoring: yes, without database logging
Environment Monitoring: yes, without database logging

Eligible for email and telephone support: no
Eligible for support at http://forums.netikus.net: yes

⚠️ All configuration settings are retained when upgrading from EventSentry Light to EventSentry.
2 Installing EventSentry

The installation of the EventSentry agent

- does not require a reboot in most cases
- occupies approximately 100Mb of disk space in the %SYSTEMROOT%\system32\eventsentry directory
- supports the MSI format for easy Active Directory integration

You can install and manage remote agents through with the EventSentry Management Console, using the remote update feature. Please see Managing Agents for more information.

The destination directory for the services cannot currently be changed. All necessary EventSentry service files are copied to the %SYSTEMROOT%\system32\eventsentry directory.

2.1 Requirements

Hardware Requirements
All EventSentry components, including the agents, require a Pentium IV or higher processor with SSE3 support.

Operating System Platforms
EventSentry runs on the following platforms:

<table>
<thead>
<tr>
<th>Operating System Version</th>
<th>Windows Editions</th>
<th>Run Installer</th>
<th>Monitor with Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows® NT 4 SP6</td>
<td>(all versions and service packs)</td>
<td>up to EventSentry v2.90</td>
<td>up to EventSentry v2.90</td>
</tr>
<tr>
<td>Windows® 2000</td>
<td>(all versions and service packs)</td>
<td>up to EventSentry v2.92</td>
<td>up to EventSentry v3.0.1</td>
</tr>
<tr>
<td>Windows® XP SP3</td>
<td>(Home, Professional), including x64 editions</td>
<td>up to EventSentry v3.1.1</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® Small Business Server 2003 SP2</td>
<td>(all service packs)</td>
<td>up to EventSentry v3.1.1</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® Server 2003 SP2</td>
<td>(all service packs), including x64 editions</td>
<td>up to EventSentry v3.3.1</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® Vista</td>
<td>(all editions), including x64 editions</td>
<td>up to EventSentry v4.0.3</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® Server 2008 (R2)</td>
<td>(all editions), including x64 editions</td>
<td>all versions</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® 7</td>
<td>(all editions), including x64 editions</td>
<td>all versions</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® 8 &amp; 8.1</td>
<td>(all editions), including x64 editions</td>
<td>v2.93 and later</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® Server 2012 (R2)</td>
<td>(all editions), including x64 editions</td>
<td>v2.93 and later</td>
<td>all versions</td>
</tr>
<tr>
<td>Windows® 10</td>
<td>(all editions), including x64 editions</td>
<td>v3.2 and later</td>
<td>all versions</td>
</tr>
</tbody>
</table>
Installing EventSentry

Windows® Server 2016 (all editions), including x64 editions
- v3.3 and later
- all versions

Windows® Server 2019 (all editions), including x64 editions
- v3.5 and later
- EventSentry v3.5 and later

Windows® 11 (all editions), including x64 editions
- v5.0 and later
- EventSentry v5.0 and later

Windows® Server 2022 (all editions), including x64 editions
- v5.0 and later
- EventSentry v5.0 and later

See below for requirements of specific components.

Permissions
The following permissions are required to install EventSentry with the setup application:

- Administrative permissions

or

- Permission to create and control services
- Permission to write files to %SYSTEMROOT%\SYSTEM32
- Permission to write \Program Files directory
- Permission to write to the registry key HKEY_LOCAL_MACHINE\Software

Running the EventSentry installer on a Workstation-OS like Windows 10 is possible but not recommended and not supported for production use.

ADMonitor
The following are required for ADMonitor to work:

- The host where ADMonitor is installed must be a member of the domain it monitors
- The ADMonitor service account (EventSentryADMonitor) must be a local administrator and member of the Domain Admins group
- The ADMonitor service account (EventSentryADMonitor) must be a member of the Enterprise Admins group if a child domain is being monitored
- The Group Policy Management feature must be installed in order to monitor group policy changes
- Limited auditing for “Account Management”, “Directory Service Access” and “Active Directory Diagnostic Event Logging” is required to determine the user who performed a change (can be configured with administrator utility)

Collector
The following requirements are recommended for hosts running the collector service:

- Operating System: Server OS, Windows 2012 R2 or higher
- CPU: 4 or more cores
- Memory (RAM): At least 512Mb available for the collector, 1 Gb or more recommended

Network Services
The Network services service (which includes the Syslog, Snmp, ARP and NetFlow daemon) requires at least a 5-host network device license, the NetFlow component requires at least one NetFlow license.
There is no license requirement for the “Network Services” component included with EventSentry Light edition which only supports 2 remote hosts and does not support logging incoming Syslog and/or SNMP traps to a database.

**NetFlow**
The following flow protocols are supported by the EventSentry NetFlow component:

- NetFlow v1
- NetFlow v5
- NetFlow v9
- IPFIX
- sFlow

**Agent Management (Manual or MSI)**
Agents can either be installed with the management console or with MSI files. The following requirements need to be met in order to deploy and manage EventSentry agents with the management console:

- The ADMIN$ share needs to be present in order for the agent to be pushed.
- The ADMIN$ share needs to be present for configuration updates to be pushed to the agents. If the ADMIN$ share does or cannot exist, then you can setup the ES$ share instead.
- The Client for Microsoft® Networks needs to be installed

Agent-only installers can be generated by the management console (requires free WiX software) and installed or deployed to the target computers.

The collector (installed by default) can be utilized to keep the configuration as well as remote agents up to date. When using the collector, only the initial installation of the agents needs be performed (either with remote update or a MSI file).

**Web Reporting**
The EventSentry web reports support the following web browsers:

- Mozilla Firefox 65 or higher
- Microsoft® Internet Explorer 11 or higher
- Microsoft® Edge (latest version)
- Google Chrome™ 72.0.3626 or higher
- Opera 58.0.3135.47 or higher
- Apple® Safari® 12.0.2 or higher

Older versions of the above listed browsers and browsers not listed may work with the EventSentry web reports but have not been verified.

The EventSentry web reporting requires a supported database server (see “Database” below) with an EventSentry database.

**Database Requirements**
See [Database Requirements](#) for more information on ODBC drivers and supported databases.

**Hardware (optional)**
All sensors, except for the USB-only temperature/humidity sensor, require:

- One available serial port (used for data collection)
• One available USB port (used for power)

The USB-only sensor requires one available USB port as well as a USB to COM port driver from FTDI Chip. This driver is included with EventSentry and located in the “resources” sub directory of the main installation directory.
2.1.1 Hardware Specifications for Sensors

Hardware specifications for environment sensors manufactured by PCMeasure:

**Sensor 30101 (temperature only)**
- Temperature Range: -30 to 100 degrees celsius
- Absolute fail in this range: +/- 1.2 K
- Non-linearity: 0.4 K
- Length: 28 mm
- Diameter: 8.5 mm
- Material: Ertacetal C
- Cable: 1.5 meters PVC, diameter 3.2 mm
- Environment: for use in air

**Sensor 30106 (temperature and humidity)**
- Temperature range: -30 to 80 degrees celsius
- Absolute fail in this range: +/- 1.2 K
- Non-linearity: 0.4 K
- Humidity range: 0 to 100% relative humidity
- Humidity accuracy: +/- 3.5% in range 20-80% humidity
- Dimensions: 60 x 58 x 25 mm
- Environment: for use in air (inside)
- Additional Information: Device has a Sub-D9 and USB connector and features a RJ 45 connector which supports an additional cable for a total length of up to 100 meters

2.1.2 Databases

**Database ODBC Drivers**

When consolidating data to a central database, then the appropriate database ODBC drivers will need to be installed on the host where EventSentry is installed (when utilizing the collector), or on each client that is to write to the database. No action is required when using a MSSQL Server database with Windows® 2003 (or newer) hosts, but please see the table below for more information on which ODBC drivers need to be installed.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL</td>
<td>included with EventSentry installation</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2005-2017</td>
<td>included with Operating System, but latest driver recommended for server-side components</td>
</tr>
</tbody>
</table>

Support for MySQL will likely be phased out in future versions of EventSentry. Current users of either database are highly encouraged to migrate to a different database.

**Database Support Tiers**

EventSentry supports 3 different types of SQL database servers: PostgreSQL, Microsoft® SQL Server and MySQL (to be phased out). EventSentry offers different support levels depending on the type and version of the database. These different support levels are described by their respective database tiers, shown below:
### Tier Level Description

<table>
<thead>
<tr>
<th>Tier Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 (recommended)</td>
<td>Database is fully supported and has undergone extensive testing.</td>
</tr>
<tr>
<td>Tier 2</td>
<td>Database is supported and has undergone basic testing.</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Database is compatible with EventSentry but not officially supported and has only undergone minimal testing. Use this database only if you have experience with it.</td>
</tr>
</tbody>
</table>

### Database (optional)

A database server is required for the web-based reporting, and when consolidating event logs, system health and other information in a central database. Not all database types and versions are supported equally, the database support tier (see "Database Support Tiers" above) describes the support level of the database.

<table>
<thead>
<tr>
<th>Database</th>
<th>Support Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL 9.1</td>
<td>3</td>
</tr>
<tr>
<td>PostgreSQL 9.6</td>
<td>2</td>
</tr>
<tr>
<td>PostgreSQL 14</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2008 (32-bit or 64-bit)</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2008 Express</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2008 R2 (32-bit or 64-bit)</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2008 R2 Express</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2012</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2012 Express</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2014</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2014 Express</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2016</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2016 Express</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2017</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft® SQL Server 2019</td>
<td>1</td>
</tr>
</tbody>
</table>

### 2.2 Getting EventSentry

To obtain the latest version of EventSentry from our website please follow the steps below:

- Navigate to the **Downloads** section of [http://www.eventsentry.com/](http://www.eventsentry.com/) and follow the **Download Now (registered users only)** link, or access the customer area at [https://store.netikus.net/customer/](https://store.netikus.net/customer/)

- Follow the instructions on this page, you will be required to login with your email address and password

- You will see a window similar to the one shown below. Click on **Download** to download the latest version.
• Install the software. The setup program will update the existing installation and preserve the configuration.
2.3 Licensing EventSentry

EventSentry requires a valid license to run, currently we have trial and full licenses available. EventSentry Light does not currently require a license.

License keys can either be loaded from a file (during installation and in the management console), or pasted into the license manager in the management console.

Since all monitored machines need a valid license, you can use remote update to send license information to all monitored machines. Licensing information is automatically updated when you perform the following remote update features:

- Update Configuration
- Upgrade Agent(s)

Note that you will need to restart the agent in order to reread the license information. This is particularly important when switching from a trial to a full license.

Trial License

A trial license allows you to evaluate EventSentry for a limited amount of time so that you can determine whether it fits your network monitoring needs. The evaluation period is currently 30 days and may be extended by contacting NETIKUS.NET Sales.

You can request a trial period for EventSentry by navigating to http://www.eventsentry.com/downloads/trial and filling out the trial request form.

When you have completed your evaluation of EventSentry then you can purchase the full version. Upon completion of your purchase you will receive a license key to permanently activate your trial version so that EventSentry will not expire.

Full License

The full license allows you to use EventSentry on as many computers as you purchased licenses for. Full licenses do not expire, however support and updates expire one year after the original purchase date.

Full (Agent) Licenses

Full agent licenses are required for each host running Microsoft Windows where you want to monitor the event log and/or system health. Monitoring the event logs and system health require the use of an agent, hence the license type is Agent.

Network Device Licenses

You can use network device licenses when you are monitoring hosts through the heartbeat or network services feature but are not installing the EventSentry agents on those machines. This applies to Unix/Linux computers as well as network devices like routers, switches etc..

⚠️ The network services service requires at least a 5-host heartbeat / network device license.

Syslog & SNMP Licensing Details

When a network device sends Syslog or SNMP data to EventSentry, it will use one license for a minimum of 24 hours from the last time the device sent data. If that device does not send any additional data for 24 hours or more, that license will be made available to other network devices sending data.

NetFlow Licenses
The NetFlow component is part of the network services but licensed separately. In order to utilize NetFlow, a NetFlow license needs to be installed for every NetFlow collector installed/enabled. For example, if you have 2 routers sending NetFlow data to the same EventSentry NetFlow collector, then one NetFlow license is required.

See the next chapters for information and screenshots on how to correctly enter license information.

2.3.1 Entering a License

When you start EventSentry for the first time then you will see the licensing dialog as shown in the dialog below. The Trial Version Information area shows how many days are left for evaluation (or indicates that you are running the full version) and you can enter a new or update an existing license with the Manage Licenses button.

**Important information about licenses**

1. You can only install a maximum of one trial license.
2. All installed licenses must have the same organization name.
3. All installed licenses must have the same version number (see below)
4. You will need to have at least one regular (agent) license installed, EventSentry will not work if you only have network device licenses or NetFlow licenses installed.

**Version Numbers and Expiration**

All licenses are perpetual and will never expire, but will only work with versions of EventSentry which were released before the expiration date of the installed licenses.

**Example**

You cannot install a version of EventSentry which was released on May 1st 2019, if the installed licenses expire on April 1st 2019. You are however eligible to install any version of EventSentry which was released on or prior to April 1st 2019.

The expiration date of a license reflects the end of the maintenance agreement. Renewing the annual maintenance and thus extending the maintenance expiration date will result in new license keys being generated and sent to the user. These license keys can easily be imported into the management console.
Managing Licenses
After clicking the Manage Licenses button you will be presented with the License Management dialog:
The license management dialog lists all installed licenses (up to 25 licenses are supported) and shows the total number of installed licenses, including how many licenses are still available (Total Available Licenses).

To add a new license, click the Add button. To remove a license, click the Remove button. You can view an already installed license by clicking the View button.

Adding Licenses
Licenses can either be added individually with the Add button, or imported in bulk from a file with the Import button (recommended).

Importing licenses
When a license file is available, importing the entire file with all license keys contained within the file is the easiest way to add licenses. License files are sent from the NETIKUS.NET Online Store whenever a maintenance agreement is renewed or when new licenses are purchased. Importing licenses will replace all existing licenses with the licenses from the license file.

Adding a license
To add an individual license, click the Add button and paste the license key into the License Information dialog shown below.

Paste the entire license key **exactly as it appears in the email or the license file**. If the key is valid then it should automatically validate and fill in the license details on the bottom. Clicking the **Validate** button will manually attempt to validate the license key.

A validated license key will show similar to the dialog shown below:
2.4 Local Installation (with installer, default)

To install EventSentry with the installer, simply run the downloaded installer package, for example eventsentry_v4_1_1_0_windows_setup.exe. The following optional components are available:

**Help**
Installs the complete documentation as well as additional guides on the local computer in HTML format. Additional formats are also available on the product web site at https://www.eventsentry.com/support/documentation.

**Built-In Database**
EventSentry supports different databases, including the default PostgreSQL database that ships with the product. Select this component to install an instance of PostgreSQL on the local computer (recommended).

When selecting this component, the following options are available:

- **Folder**: Specify where the database will be stored. **Select a drive/directory with sufficient space**.
- **Firewall**: Specify whether setup should add a firewall rule to allow incoming traffic to the local database (port 5432). Generally not required when using the collector.
- **Admin Password**: Specify the password for the administrative postgres user. It is highly recommended that you choose a secure password.

Choose a secure password for the administrative postgres user, it has full access to all data.
Web Reports
The web reports are the reporting interface to the database. The web reports can either be installed as part of the setup or installed separately (e.g. to install them on a different host). When this box is checked then the web reports will be installed as part of the main installation (default).

**Port:** Specify the default port the web reports will run under (8080 by default)
**Service Port:** Specify the service port the web reports will use. This port is only accessible on the local machine (8081 by default)
**Firewall:** Specify whether setup should add a firewall rule to allow incoming traffic to the web reports (port 8080 by default)

When the installation is complete, the Configuration Assistant will be launched and customize the default installation. It will setup the default email notification, finalize the database setup and allow you to configure Syslog, SNMP and other features.

2.5 Updating to a new version
EventSentry is constantly under development and new versions are available for you to download from our website. Please read the next chapters on how to update EventSentry. EventSentry comes with free updates for one year, additional years of support and updates are available for a yearly fee. Please check our pricing web page for more information on current pricing.

If you already installed EventSentry, then you can easily check for a new version by navigating to Help -> Check for Updates, or visit http://www.eventsentry.com/downloads/version-history.

If you are a registered customer with an active maintenance agreement then please see Getting EventSentry for instructions on how to download the latest version.

2.5.1 Updating to v5.0
EventSentry v5 introduces two major changes with a more complex upgrade process compared to previous upgrades, especially for users utilizing the built-in PostgreSQL database.

Running the latest EventSentry installer will update an existing installation to the latest 5.0..x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and optionally back up your database.

All server-side components of EventSentry, including the installer, built-in database and all utilities are now 64-bit. Agents are still available for 32-bit systems, but EventSentry can only be installed on 64-bit systems.

EventSentry now ships with the 64-bit version of PostgreSQL v14. This latest version of PostgreSQL includes a number of improvements that will make the built-in database faster and more reliable. Upgrading to v14 is not required but highly encouraged.

Several migration options will be available, see below for more details.

Clear text connections to the collector will be phased out in the next release of EventSentry. Users utilizing clear text connections with the collector need to migrate to TLS connections.
64-Bit Upgrade

Main Files
As part of the installation process, all user data (e.g. MiBs, configuration backups) will be moved from the existing installation directory (e.g. `C:\Program Files (x86)\EventSentry`) to the new 64-bit installation directory (e.g. `C:\Program Files\EventSentry`). Any custom directories and files located in the 32-bit installation folder should be backed up and manually moved to the new installation directory.

After removing binary and temporary files (e.g. installers, crash dumps), the 32-bit installation directory will be compressed into the `backup_eventsentry_x86.zip` zip archive (in the 64-bit installation folder).

ADMonitor
Since ADMonitor binaries from version 4.2 and earlier are 32-bit and have also been migrated to the 64-bit platform, all data associated with ADMonitor will also be migrated to the 64-bit installation folder. All 32-bit ADMonitor data will be moved to the 64-bit installation directory and compressed (stored in the `ADMonitor\backup` sub directory) for backup purposes.

PostgreSQL Upgrade
When an existing PostgreSQL 9.6 database is detected, then the installer will prompt the user on whether to install the newer v14 PostgreSQL database.

Upgrading from EventSentry version 3.2 or earlier, which uses PostgreSQL 9.1 is not supported. Users wishing to upgrade to version 5.0 should either first upgrade to EventSentry 4.2 or contact support for additional options.

The following two options are available when installing PostgreSQL v14:

Option 1: Archive existing data in PostgreSQL v9.6, store new data in PostgreSQL v14
Existing data is preserved in PostgreSQL v9.6, but all new data is stored in the updated v14 database. The existing v9.6 database will continue to run and will be accessible via an "Archive" profile in the web reports. New data will be accessed the same way as before. This is the most simple approach with the shortest downtime, and is recommended for large v9.6 databases.

Option 2: Migrate existing data to PostgreSQL v14, retire v9.6
Runs a script that copies data from the existing v9.6 database to the updated v14 database utilizing the PostgreSQL `pg_dumpall` utility. EventSentry services will be unavailable during the migration, and this process is potentially time consuming (depending on hardware and the size of the database). Since this process copies data from one database to the other, it requires free disk space equivalent to the size of the existing 9.6 database. This option does eliminate the need to keep the existing v9.6 database but is generally only recommended for smaller databases.

See the diagram below for an overview of the pros and cons of each option:

<table>
<thead>
<tr>
<th>Keep PostgreSQL v9.6 database to access old data</th>
<th>Option 1 (no data migration)</th>
<th>Option 2 (data migrate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to run searches &amp; reports against old &amp; new data in web reports</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Potentially extended EventSentry downtime</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Potential for errors during data migration</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Requires free disk space based on existing database size</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

Updating from v3.5 and v4.x
No specific instructions, run installer.

**Updating from v3.4**  
Version 3.5 and later ship with a 64-bit version of the EventSentry Heartbeat Monitor, the configuration assistant will automatically upgrade an existing 32-bit heartbeat service during the post-setup process.

**Updating from v3.3**  
Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

**Updating from v3.2**  
A direct upgrade path from v3.2 is not supported. In order to upgrade to version 5.0 users will need to upgrade to version 4.2 first and then upgrade to version 5.0.

### 2.5.2 Upgrading to v4.2

Running the latest EventSentry installer will update an existing installation to the latest 4.2.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and optionally back up your database. After the setup has completed and all files are updated the configuration assistant will update all configured databases to the latest schema.

Future versions of the EventSentry installer may only support 64-bit platforms. 32-bit platforms can still be monitored with the agent, but all server-side components will only support 64-bit systems. It is recommended to move EventSentry installations to a 64-bit platform in anticipation of this change.

Support for MySQL has been phased out in v4.2 of EventSentry. Current users of MySQL are highly encouraged to migrate to a different database. See Database for more information on supported database types and versions.

**Updating from v4.0 and v4.1**  
No specific instructions, run installer.

**Updating from v3.5**  
No specific instructions, run installer.

**Updating from v3.4**  
Version 3.5 and later ship with a 64-bit version of the EventSentry Heartbeat Monitor, the configuration assistant will automatically upgrade an existing 32-bit heartbeat service during the post-setup process.

**Updating from v3.3**  
Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

**Updating from v3.2**  
Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

**Updating from v3.0 or v3.1**
Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.

**Updating from v2.9x**
When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to “Updating from v3.0” listed above.

### 2.5.3 Updating to v4.1
Running the latest EventSentry installer will update an existing installation to the latest 4.1.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and optionally back up your database. After the setup has completed and all files are updated the configuration assistant will update all configured databases to the latest schema.

This update adds additional columns to the Syslog table to support acknowledging Syslog messages. On installations with a large amount of Syslog data the post-update process may take much longer than usual, depending on the database performance and amount of Syslog data present.

Future versions of the EventSentry installer may only support 64-bit platforms. 32-bit platforms can still be monitored with the agent, but all server-side components will only support 64-bit systems. It is recommended to move EventSentry installations to a 64-bit platform in anticipation of this change.

Support for MySQL will be phased out in future versions of EventSentry. Current users of either database are highly encouraged to migrate to a different database. See Database for more information on supported database types and versions.

**Updating from v4.0**
No specific instructions, run installer.

**Updating from v3.5**
No specific instructions, run installer.

**Updating from v3.4**
Version 3.5 and later ship with a 64-bit version of the EventSentry Heartbeat Monitor, the configuration assistant will automatically upgrade an existing 32-bit heartbeat service during the post-setup process.

**Updating from v3.3**
Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

**Updating from v3.2**
Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

**Updating from v3.0 or v3.1**
Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.
2.5.4 **Updating to v4.0**

Running the latest EventSentry installer will update an existing installation to the latest 4.0.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and optionally back up your database. After the setup has completed and all files are updated the configuration assistant will update all configured databases to the latest schema.

**Updating from v3.4**

Version 3.5 and later ship with a 64-bit version of the EventSentry Heartbeat Monitor, the configuration assistant will automatically upgrade an existing 32-bit heartbeat service during the post-setup process.

**Updating from v3.3**

Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see [KB 370](#) for more details.

**Updating from v3.2**

Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

**Updating from v3.0 or v3.1**

Version 3.2 introduced the new collector component, see [Collector](#) for more information. Also see updating from version 3.2 and v3.3 above.

2.5.5 **Updating to v3.5**

Running the latest EventSentry installer will update an existing 3.x installation to the latest 3.5.1 build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema and update the local heartbeat agent (if installed) to 64-bit. See below for additional details.

**Updating from v3.3 and later**

Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see [KB 370](#) for more details.

**Updating from v3.2**

Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

**Updating from v3.0 or v3.1**

Version 3.2 introduced the new collector component, see [Collector](#) for more information. Also see updating from version 3.2 and v3.3 above.
Updating from v2.9x
When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.6 Updating to v3.4
Running the latest EventSentry installer will update an existing 3.x installation to the latest 3.4.1 build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. See below for additional details.

Updating from v3.3
Version 3.4 ships with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

Updating from v3.2
Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

Updating from v3.0 or v3.1
Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.

Updating from v2.9x
When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.7 Updating to v3.3
Important Changes
EventSentry v3.3 introduces two major changes which impact the upgrade process more than previous updates:

- A new built-in database, PostgreSQL v9.6, ships with v3.3
- A 64-bit EventSentry agent is now available

PostgreSQL v9.6
Since (security) updates no longer available for the previously included PostgreSQL v9.1 database, EventSentry now ships with a newer version of PostgreSQL. Upgrading an existing database is not required, see KB article 332 which outlines all available upgrade options. For users utilizing the legacy built-in database, it is recommended to install the new v9.6 database, even if it will not be utilized immediately.

64-Bit Agent
A 64-bit agent is now available for hosts running a 64-bit version of Windows. A 64-bit agent makes it possible that 64-bit performance counters can be read from the agent, and that accessing 64-bit OS files (e.g. C:\Windows\System32) no longer requires disabling FS redirection. Please note that not all EventSentry components will be 64-bit, for example the management console is still a 32-bit process (although a 64-bit version is available).

Updating from v3.x
Running the latest EventSentry installer will update an existing 3.x installation to the latest 3.3.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. No further action is required.

**Updating from v2.9x**

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

### 2.5.8 Updating to v3.2

**Updating from v3.0 and 3.1**

Running the latest EventSentry installer will update an existing 3.0.1 or 3.1.1 installation to the latest 3.2.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. No further action is required.

**Important:** Version 3.2 includes the new “collector” component which can either be activated during the upgrade with the configuration assistant or installed and configured after the upgrade is complete. See Collector for more information.

**Updating from v2.9x**

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

### 2.5.9 Updating to v3.1

**Updating from v3.0**

Running the latest EventSentry installer will update an existing 3.0.1 installation to the latest 3.1.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. No further action is required.

**Updating from v2.9x**

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

### 2.5.10 Updating to v3.0

The biggest change when updating to version 3.0 from any earlier version are the new web reports which no longer require IIS. The new web reports run on Windows, Linux and Apple OS X and utilize Java on the server side (included with the EventSentry installation). The new web reports also ship with their own web service. The existing web reports (referred to as the “Legacy Web Reports”) will not be uninstalled by the 3.0 upgrade, refer to this KB article for instructions on how to uninstall.

Version 3.0 includes an improved filter scheduling feature, with the ability to setup more granular recurring & summary filters. We recommend that you review the "Hour/Day" tabs on all filters which have custom settings configured in that tab.

**Web Reports**

The new web reports include a variety of new functionality, including the following:
UTC support for networks spanning multiple time zones
Built-in web service which no longer relies on IIS
Cross-platform capabilities for Linux and OS X support
Ability to schedule & email reports
Improved search capabilities for complex search queries
PDF output

Java is not required on the client side - only on the host where the web reports are running.

SNMP Polling (Heartbeat Monitoring)

The heartbeat agent includes the ability to query SNMP counters from SNMP-enabled hosts through the existing performance monitoring feature. In addition to polling counters, the HB agent can also query disk space, uptime and basic hardware / OS information.

Ribbon (Management Console)

The management console offers a redesigned interface featuring the ribbon as well as updated icons throughout the interface. The following new features have also been added:

- Support to view application and services event logs with the build-in event viewer
- Better interface to configure day/time schedules, summary & recurring event filters
- Recurring events can now be configured to check minutely intervals
- Authentication has been redesigned so that credentials are created & applied to hosts or groups
- Misc usability improvements throughout the management console

Monitoring

- Log file monitoring supports sub folders
- Compliance "Logon By Type" tracking can exclude logons by computer accounts
- Event Log filters can override email subject & message body
- Packages can be dynamically assigned based on platform (32bit vs 64bit)
- Threshold filters can utilize insertion strings
- Disk space prediction feature (predicts when disk will be full)
- Identify reasons why hosts were shut down or rebooted
- Desktop notification supports Growl
- Network notification supports remote desktop services
- Application scheduler support process isolation
- New email format "HTML Modern"

Network Services

The network services include a new "ARP" daemon, which monitors network traffic and alerts users when new MAC addresses are found or MAC to IP associations change. The ARP daemon also keeps track of all significant MAC address changes and the current status of all MAC addresses and their IP associations can be reviewed through the web reports.
2.5.11 Updating from v2.7x to v2.90

Please follow these steps to update from EventSentry version 2.7x / 2.8x to version 2.90.

1. Just in case there are problems with the update, export the configuration using the File -> Export function of the management console.

2. Run the EventSentry 2.9x installer on the same machine where you previously ran the installer. You should not be prompted for license or setup information. The same setup options that were selected when you installed the previous version of EventSentry should be automatically selected. If not, then please ensure that the same settings are selected.

3. If you are currently using a MSSQL or MySQL database then make sure that you select the respective option on the Custom Setup page of the setup when you update. This ensures that all tables in the EventSentry database are updated, a requirement before you can update the agents.

4. A reboot is generally not required, but might be necessary depending on the OS you are using and other dynamic factors.

5. Once the setup is complete and the database has been updated (if the ESOBJECTTRACKING table exists in the EventSentry database then you know that you are database has been updated) you can start pushing out the updated agent.

Navigate to Remote -> Update Agent(s) to push the new agent to all remote monitored machines.

2.5.12 Updating from v2.60 to v2.70

This chapter contains very important information for users updating to version 2.7x from earlier versions of EventSentry. Read this chapter carefully to avoid losing parts of your configuration.

Local Filters

With the introduction of filter packages, the previously introduced Local Filters feature has become obsolete and will not be supported anymore. While local filters will be migrated to a "Local Filters Package" on the computer where you run the EventSentry setup, they will be lost on remote computers that are updated with the remote update feature.

Local filters from version 2.60 (and earlier) will be lost the first time you update the remote agents or push the configuration.

If you need to retain the local filters that you created on remote computer then you will have follow the steps below:

1. Connect to the remote computers that have local filters and note down the names and properties of these filters, including the computer name.
2. After you have migrated to version 2.70 create a filter package, for example "Custom Filters".
3. Add all the filters to this package, and make sure that enter the computer name where these filters are from in the Computer Name field. This will ensure that the filter will only be processed on that computer.
4. Make the package global or assign it to all computers that had local filters in version 2.60.
Global Filters
With the introduction of filter packages, the previously introduced Global Filters feature will not be available anymore, instead you can create global packages that will be processed on all computers. Global filters will be automatically migrated to a Migrated Global Filters package when updating to version 2.70.

Packages
Starting with version 2.70, filters are not organized through groups, global and local containers anymore. Instead, filters are organized into filter packages which are then assigned to either groups or computers. Filter packages can also be made global so that they apply to all computers, regardless of group membership.

Your configuration will of course be preserved, and all filters that previously belonged to a group will be automatically migrated to a package. For example, all filters from the SERVERS group will be migrated to Migrated filters from SERVERS. Health and tracking packages are now also organized using packages, and will migrated in a similar fashion.

We recommend that you review your configuration after the migration carefully and make adjustments as necessary. For example, you will almost always be able to consolidate your health packages into one or two packages.

Filter package order is not relevant for package/filter processing. Exclude filters will always be processed before include filters, regardless of their package order.

Database
Since new tables were added to the database it is also necessary to update the database. If you are using Microsoft® SQL Server, then you database will be automatically updated during the installation, make sure that you select the database feature and provide login information.

If you are using MySQL, Oracle or Access then you will need to update the database using the Database Setup Wizard. Running the Database Setup Wizard after the installation has been updated will ensure that all necessary tables exist.

Upgrading from EventSentry v2.60 to v2.70 (or later)
1. Download the most current setup file and start the installation on the machine where the management console is installed. You will not have to apply any patches if you download the latest setup, which already has all patches incorporated into it.

2. The MSI installer will now automatically upgrade your existing installation. If the upgrade fails, uninstall version 2.60 (make sure you have a configuration backup) and then run the latest setup again. If your configuration was not preserved, import the previously exported configuration (File -> Import).

3. Perform a Remote Update “Manage Agent(s)” to update the service on the remaining computers, and ensure that "Always update configuration when updating remote agents" is checked in Tools -> Options -> Remote Update. Read the Local Filters section above as local filters on remote computers will be discarded when you update the configuration on remote hosts.

2.5.13 Updating from v2.50 to v2.60
Please follow the instructions below to update all EventSentry installations in your network. Always make sure that you export the configuration prior to any version upgrade.

Upgrading from EventSentry v2.50 to v2.60 (or later)
1. Download the most current setup file and start the installation on the machine where the management console is installed. You will not have to apply any patches if you download the latest setup, which already has all patches incorporated into it.
2. The MSI installer will now automatically upgrade your existing installation. If the upgrade fails, uninstall version 2.50 (make sure you have a configuration backup) and then run the latest setup again. If your configuration was not preserved, import the previously exported configuration (File -> Import).

3. Perform a **Remote Update "Manage Agent(s)"** to update the service on the remaining computers.

**Upgrading from EventSentry v2.43 (or earlier) to v2.50 (or later)**

1. Uninstall the currently installed version from the template (management) machine and make sure that you keep the configuration.

2. **MySQL and Oracle only:** Run the Database Setup Wizard to initialize the new EventSentry database.

3. **Optional:** Run the Database Migration Wizard to migrate data from the existing to the new database.

4. **Configure new features and save the configuration.** It is recommended that you change ODBC actions to use connection strings instead of System DSN names.

5. Perform a **Remote Update "Manage Agent(s)"** and update the service on the remaining computers.

**Upgrading from EventSentry v2.x to v2.43 (or earlier)**

1. Download the most current setup file (eventsentry_v2.XX_setup.exe). Run the setup on all template (management) machines. An uninstall of the current version is not required. A reboot is not required.

2. **Configure new features and save the configuration.**

3. Perform a **Remote Update "Update Configuration"** and update all settings.

4. Perform a **Remote Update "Manage Agent(s)"** and update the service on the remaining computers.

**Upgrading from EventSentry v1.x to v2.30**

1. If EventSentry Light v1.x was installed with the installer then uninstall it first.

2. Install the 2.x version of EventSentry on the management computer in your network; the existing service will be stopped and updated, the configuration will be preserved.

3. If applicable remove all left over files that belong to EventSentry v1.x (e.g. eventsentry_gui.exe)

4. Launch the management interface and verify that the configuration was converted correctly.

5. **Configure new features and save the configuration.**

6. Perform a **Remote Update "Update Configuration"** and update all settings.

7. Perform a **Remote Update "Manage Agent(s)"** and update the service on the remaining computers.
2.5.14 Upgrading from EventSentry Light

If you have purchased EventSentry after evaluating EventSentry Light then you will need to upgrade all EventSentry Light installations.

To upgrade to EventSentry after using EventSentry Light you will need to upgrade one computer manually (1. below) and then, if you have multiple installations, perform a remote update (2. below). You can also update the service manually on each computer if you wish.

1. On the Local (template) Machine

1. If you are upgrading from EventSentry Light Version 1.x and installed it with the installer then you will need to uninstall EventSentryLight v1.x first. Otherwise just skip this step.
2. Install EventSentry with the setup program.

2. On Multiple Remote Machines

1. Make sure that the computer from which you are performing the remote update has the latest and full version of EventSentry installed (see above).
2. Add all the computers you wish to update to the remote update - either manually or by importing them.
3. Choose Update from the Manage Agent(s) submenu.
4. The service on the remote machines will be stopped, the service executable updated, and the service restarted. Please note that the service will only be restarted on the those computers where the service was running.

2.5.15 Upgrading from the EventSentry Trial Version

If you have purchased EventSentry after evaluating the trial version of EventSentry then you will need to update the license information on all EventSentry installations. A reboot is not necessary.

To upgrade to EventSentry after using the trial version of EventSentry you will need to upgrade one computer manually (1. below) and then, if you have multiple installations, perform a remote update (2. below). You can also update the licensing information manually on each computer if you wish.

1. On the Local Machine (Management Workstation)

1. Enter your full license by launching the EventSentry License Management which can be found in the Program Files folder.

2. On Multiple Remote Machines

1. Make sure that the computer from which you are performing has the full license configured.
2. Add all the computers you wish to update to the remote update.
3. Right-click the **Groups** node in the left pane and select **Remote Update -> Manage Agent(s) -> Update**. Alternatively you can also right-click the **Computers** node in a selected group and select **Manage Agent(s) -> Update**.

4. The service on the remote machines will be stopped, the service executable and license information updated, and the service restarted. Please note that the service will only be restarted on the those computers where the service was running.

### 2.5.16 Advanced Users

The following two chapters outline how to perform advanced update functions usually only necessary when troubleshooting EventSentry. Most users can skip these chapters.

#### 2.5.16.1 Manually updating the Service

This section describes how to update the EventSentry **services** manually.

**On the Local Machine**

The service for the local agent, heartbeat service, collector and/or network services can be manually updated. Depending on the component that requires an update, click on one of the following icons in the left tree:

- Services
- Collector
- Heartbeat
- Network Services

Then, click the **Update button** on the component's dialog. You will be prompted to point to the folder where the new version of the service will be located.

![Continue updating service? dialog]( Continue updating service? 

The service will now be stopped and the service executable replaced, continue?

[Yes] [No]

After you confirm the dialog box with **Yes** the

- service will be stopped
- the service executable will be replaced
- and the service will be restarted (if it was running before the update)

**On Multiple Remote Machines**

1. Make sure that the computer from which you are performing the remote update has the latest version of the service installed or access to the latest service executable.
2. Add all the computers you wish to update into the appropriate group(s).
3. Right click "Computer Groups" or the group that requires an update and select "Manage Agent(s) -> Upgrade".
4. The service on the remote machines will be stopped, the service executable updated, and the service restarted. Please note that the service will only be restarted on the those computers where the service was running.

2.5.16.2 Manually updating the GUI and documentation

This section describes how to update the EventSentry GUI, message file and the documentation.

Management Console (GUI)
To update the management console, replace `eventsentry_gui.exe` with the updated version of the archive.

Messagefile
To update the messagefile replace `%SYSTEMROOT%\system32\eventsentry_svc_x64.exe` with the updated version of the archive. Please note that you will need to close all applications that lock the event log, such as the native Windows event viewer prior to replacing the messagefile.

On Windows Server 2003 you will need to stop/start or pause/continue the WinMgmt service prior to replacing `eventsentry_svc_x64.exe`. Restart the service after you have updated the file.

Documentation
To update the documentation replace `eventsentry_hlp.chm` with the updated version of the archive. The helpfile should always be in the same directory as the GUI `eventsentry_gui.exe`.

2.6 Moving EventSentry to a new server

If you installed EventSentry on one server/workstation and want to migrate the installation, including the management console and its settings to a new machine, then follow the steps below.

Please note that these instructions do not include instructions for moving the database to a different database server. Please see your database manual for more information on how to move a database.

1. Backup the configuration with the management console through the Home -> Export menu. This will create a .reg file that contains your entire EventSentry configuration. We will refer to this file as `ESConfigBackup.reg`. Save this file in the installation directory of EventSentry, `C:\Program Files (x86)\EventSentry` by default.

2. If you setup credentials on one or more groups or computers, then start the registry editor `regedit.exe`, navigate to `HKEY_CURRENT_USER\Software\netikus.net\EventSentry` and backup this key by right-clicking it and selecting `Export`. Save this file as `ESUserConfigBackup.reg`.

3. Make a backup copy of the EventSentry installation directory or zip the directory into an archive, e.g. `EventSentry.zip`.

4. Copy this archive or the entire folder to the target computer into a temporary folder, we suggest that you keep this file/folder for a few weeks before you delete it.

5. On the new machine, double-click the `ESConfigBackup.reg` file to import the settings into the registry.

6. Start the setup on the new machine and proceed to the `Custom Setup` dialog which allows you to select the features that are to be installed.
7. Do not select any of the database features unless you plan on setting up a new database instance from scratch on the machine, such as setting up a new Postgres instance for your new server. The existing database settings will be used on the new machine.

8. If you are migrating the web reports to the new machine as well then make sure that **EventSentry Web Reports** feature is selected.

9. Proceed with the installation, and during the Configuration Assistant phase select any of the other features that are needed in your environment, such as Heartbeat Agent, Network Services, Collector, and so forth.

10. If you are moving the web reports as well, then copy the `C:\Program Files\EventSentry\Webreports\conf` folder from the old machine to the new machine after the installation is finished. Restart the EventSentry Web Reports service on the new machine.

11. If you exported the user configuration in step 2 then double-click the `ESUserConfigBackup.reg` file in Windows explorer to import those settings.

12. If you moved any of your infrastructure that is used by one or more actions (e.g. SMTP server, database server, etc.) then ensure that you are updating the respective actions, so that they point to new location. Click the Test button in the action settings to ensure that the new server can connect to the modified action destination.

13. If you are using the collector service and moving that to the new machine as well (as is usually the case), then update the collector host name to reflect the new host name in the collector dialog in the management console.

14. If you made any configuration changes then make sure that you are pushing the latest configuration to the monitored hosts. If you modified any action settings, you'll also need to restart the local components (Home > Services) and, if not using the Collector, restart all of the remote agent services (Groups > Other Actions > Restart > Go) for the new action settings to take effect.

15. If you have any Syslog or SNMP Trap senders then you will need to reconfigure them to send to the new server.

You should at this point be ready to manage your EventSentry settings as usual.

### 2.7 Remote Agent Installation

You can install the EventSentry agent on remote machines in several ways:

**Remote Update**

The **preferred and easiest** way to install the EventSentry agents on remote computers is to use **remote update**. With remote update you can install agents, update them to the latest version or push the latest configuration. See below if you are using the "Collector" service.

**EventSentry MSI**

If the monitored computers are part of an Active Directory environment or if you are running other software that supports the deployment of MSI files, then you can create an [EventSentry Agent MSI file](#) and deploy the EventSentry agent in this way. This option might be preferable if you do not have access to the ADMIN$ share of the monitored computers. Please note that the free [WIX Toolset](#) is required to generate a MSI package for deployment in your network. [Click here](#) for more information.

**Collector**
Once the agents are deployed (either via the management console or with MSI files), the collector can patch the remote agents to the latest version and also automatically transfer the latest configuration (more info).

The default administrative share ADMIN$ (which shares the %SYSTEMROOT% directory) will need to exist in order to deploy the agents with the management console.

### 2.7.1 Deploying the EventSentry Agent MSI

In most cases you will want to initially deploy the EventSentry agent using the remote update feature of the management console, this however requires that the remote hosts have SMB file sharing enabled, that the ADMIN$ share exists, and that the user running the Management Console has rights to add new files to the remote ADMIN$ share.

If your network infrastructure does not fulfill these prerequisites or if you prefer to deploy the agent using an MSI file then you can follow the instructions here to prepare an MSI file. You can then use any software capable of deploying MSI files to install the agent on remote machines. Once the agents have been deployed successfully you can use the management console to push configuration updates using only the ES$ share, which does not require the ADMIN$ share or administrative permissions.

EventSentry utilizes the WIX Toolset to generate MSI files, as such the free WIX Toolset needs to be installed before a MSI package can generated.

Follow the steps below to generate MSI files. Please note that both 32-bit and 64-bit MSI files will be generated by the management console, and will need to deployed accordingly based on the corresponding target platform.

1. Open the management console and click on "Computer Groups"
2. On the ribbon, click "Agent Deployment" on the right hand side
3. In the resulting dialog, select "Create MSI".

4. If the WIX Toolset is not installed, you will be prompted to install it at this time. Otherwise, the management console will generate both a 32-bit and 64-bit MSI installer MSIs and store them in the deployment\msi sub directory of the EventSentry installation directory.

2.8 Web Reports

The web reports are the reporting tool for all data collected by EventSentry and require that one or more EventSentry databases are setup.

The web reports can either be installed as part of the main EventSentry setup (recommended), or downloaded from the customer area and installed separately. When installed separately, they can either be installed on the same machine where the main setup was run, or on a different machine. The default installation directory for the web reports is C:\Program Files\EventSentry\WebReports.

1a. Installation with the main EventSentry Installer
   To install the web reports with the installer, make sure that the "Web Reports" component is selected. See Local Installation for more details on the installation process.

   You can now navigate with your web browser to the index page, e.g. http://yourserver:8080/

2b. Installation with the separate web reports installer
   To perform a manual installation of the web reports, using the separate web reports installer (e.g. eventsentry_webreports_v4_2_1_0_windows_setup.exe), download the installer from the customer area and simply run the installer.

   The stand-alone installer can be run on Windows, Linux and/or OS X. The web reports can be installed on any host which has direct access to the database.

   An installation alongside an existing EventSentry installation is also possible, but running the main installer which includes the web reports is recommended in that case. If the web reports installer was installed along side an existing EventSentry installation, then it can be uninstalled at any time.

3. Configuration Files
   All settings in the web reports are stored in XML configuration files.
- configuration.xml
  This is the main configuration file for the web reports and automatically configured during the product installation. The file contains all profiles properties as well as global settings for troubleshooting.

- preferences.xml
  This file contains all global as well as user-specific preferences.

- reports.xml
  This file contains a list of all available reports.

- jobs.xml
  This file contains a list of all configured jobs.

- users.xml
  Controls access control and, when enabled, a list of all users and groups.
3 Management Console / Utilities

You can configure all aspects of EventSentry using the management console. The management console creates and manages all the registry keys that contain the configuration for the EventSentry agents.

The management console also allows you to push the configuration to remote hosts and install the EventSentry agents on remote computers, view event logs and more.

Keyboard Navigation
The management console can be navigated with the keyboard.

- To switch from the left tree view to the right pane after an item has been selected with ENTER, hit the TAB key.
- To switch back from the right dialog pane to the left tree view, press the ALT+HOME.
- Alternatively, press CTRL+1 to jump to the left tree view and CTRL+2 to jump to the right pane.
- The ribbon can be accessed by pressing the ALT key while the focus is on the left tree view. While keeping the ALT key pressed, press the desired highlighted key.

Customizing the management console
Please click here for information on how to customize the management console to fit your needs.

Toolbar
The toolbar allows you to do perform various actions quickly with the click of button, instead of having to right-click containers or navigate through the menu. See Toolbar for more information.

Finding filters and computers
The “Find Dialog” allows you to find filters or computers based on search criteria, see Searching for more information.

3.1 Customizing

You can customize many aspects of the management console by clicking Options in the Tools menu. All options are divided into the following categories:

General
Customize click behavior and tray notifications (more).

Welcome & MyEventlog
Customize the appearance of the welcome screen and preset myeventlog.com login information (more).

Confirmations
Enable/disable certain confirmations (more).

Remote Update
Configure global remote update options (more).

Features
Hide certain features in the management application (more).

Web Reports & Proxy
Configure the web reports, external search links and proxy settings (more).
3.1.1 General

Minimize to Tray
When you minimize the application put it into the tray area rather than minimizing it to the taskbar.

Double-Click
By default a single left-click on the various objects in the left tree pane will load the object details (such as filter settings) into the right pane. You can change this behavior so that a double-click is required instead of a single left-click.

Automatically collapse unselected groups
Activating this feature will make sure that the child items (containers) from only the group that was expanded will be visible at one time. This feature is particularly useful when you have more than 2 groups and want to avoid having to collapse unneeded groups when expanding another one.

With this feature selected, every time you expand a group container (e.g. Default Group), then all other groups that are expanded at that time will be automatically collapsed.

Tray Area Notifications
This notification enables you to receive event log notifications almost immediately onto your desktop. Note that the GUI needs to be active for tray area notifications to work.

![Tray Area Notifications](image)

Tray area notifications can be configured in the following ways:

Balloon Notifications
This notification type requires Windows 2000 or higher and shows event log details in a balloon as shown in the screenshot below:

![Balloon Notification](image)

The icon represents the severity of the event record. The first string is the log in which the event occurred (the security event log in this example), and the second string shows the source of the event record (also security in this example). The rest is the actual event record message with a maximum of 255 characters.

Popup Window
This notification type works with Windows NT 4 and higher and shows event log details in a popup window, similar to the Windows Messenger application. This notification type is the most flexible and useful as it offers the following additional features:
• Configure for how many seconds the window will remain active
• Move the mouse over the window to prevent it from disappearing
• Click on the popup window to view the details of the event record

The screenshot below shows a typical popup notification:

When you click anywhere in the popup window, the event log details will be shown:
Sound Notification
In addition to or instead of the visual notifications, you can also be notified by a sound file in WAVE format. If you do not specify a sound file then a default sound will be used instead.

Click on Enable to activate sound notification; click on the icon with the loudspeaker to hear the selected sound.
The tray area notifications can also be configured by right-clicking the tray icon:

![Configuration Backup](image)

**Automatic Configuration Backup**

You can automatically backup the EventSentry configuration in regular intervals by activating this feature. Simply check the "Backup Configuration" checkbox and set a backup interval (daily, weekly or monthly). From now on, every time you start the Management Application, EventSentry will automatically backup the configuration in the **Backups** sub directory of the installation directory when necessary. Old configuration backups will automatically be purged according to your settings as well.

![Backup Configuration](image)

You will have to open the Management Application in order for the configuration to be backed up, the EventSentry agent is not backing up the configuration automatically.

### 3.1.2 Version Check / Welcome

**Version Check**

To automatically check for a **new version** every time the management console is opened, click the "Notify me if a new version of EventSentry is available" checkbox. This will automatically invoke the Check For Updates features and display the version information dialog if a new version is available.

To automatically check for **new patches**, check the "Notify me if a new patch is available" check box. If you prefer to only be notified if a critical patch has been released, also check the "Only alert me of critical patches" check box.

Enable online maintenance expiration check and integrated patch download

Allows for automatic download & installation of patches from within the management console.

**Welcome Screen**
This section allows you to customize some aspects of the welcome screen.

Display Welcome Screen on Startup
Disabling this check box will not show the welcome screen when the management interface is launched. The welcome screen will still be displayed when you manually click on the root computer icon.

Fetch news from http://www.eventsentry.com
Disabling this checkbox will not download the current news from the Internet. Disable this check box if your computer is not connected to the Internet to avoid a delay in the application startup.

If your machine is connected to the Internet then it is recommended that you active this check box as you will receive important information about new developments around EventSentry.

Event Log Viewer
This section allows you to customize features of the event log viewer.

Remember remotely connected event logs
When you connect to a remote event log using the built-in event log viewer, then those connected event logs are not reopened by default when you restart the EventSentry management console. If you enable this option however then remote event logs will be remembered and re-opened automatically.

Make EventSentry the default handler for event log backup files
In addition to opening remote event logs you can also open event log files that were previously backed up (for example by the EventSentry event log backup feature or by the Windows event viewer). If you enable this option then EventSentry will register itself to be the default application for .evt files, enabling you to double-click .evt files in explorer and view them immediately in EventSentry.

You will need to log off and log back on in order to be able to double-click the event log files in explorer.

MyEventLog.com
You can submit event log comments directly from the management application to the myeventlog.com web site. To make submitting comments faster you can setup your default profile here.

Name (Author)
Your full name. If you check the “Anonymous“ checkbox then your name will not be shown with the comments you submitted.

Email Address
Your email address is used to uniquely identify your submission. Please note that your email address will never be displayed with your postings.
3.1.3 Customizations

To avoid accidental deletions, EventSentry will prompt you before actions are taken such as before a filter or group is deleted. The screenshot below shows the available confirmation options:

![Customization Options](image)

**Test Email Customization**

When clicking the Test button in the SMTP action dialog, EventSentry sends a test email to the configured email address(es) in English. The contents of this test email can be customized. Customizing the default text can be helpful to avoid confusion or provide a translation into a local language.

3.1.4 Remote Update

**Threads**

Specify the number of threads that you would like the remote update feature to use. The more threads you use, the faster a remote update action will be performed.

A number of 5 threads is recommended for most networks, though large EventSentry installations may use a higher number to reduce the time required to perform an action such as a configuration update.

**Keep CSV log of remote update results**

Logs all remote update activity to a CSV log file, every action creates a separate file. Files are stored in the "logs" sub directory of the EventSentry installation folder, e.g. C:\Program Files (x86)
\EventSentry\logs. To access the log files, either navigate to the folder in Windows, or right-click the remote update dialog and select “View Current Log” or Browse All Logs”. The former is only available after a remote update action has completed.

**Use Checkboxes**

To selectively update only selected computers of a group you can activate this option. Instead of applying the selected action to all machines of the group(s) this will put a checkbox next to each computer object that you can check/uncheck. You can also enable/disable check boxes by right-clicking a group in the remote update:

![Use Checkboxes](image)

After you have choose one of the remote update options you will see a list similar to the one shown below:

<table>
<thead>
<tr>
<th>Host</th>
<th>Action: Check Status</th>
<th>Agent</th>
<th>Config Revision</th>
<th>SNMP</th>
<th>Ping</th>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ DB1-MYSQL56</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑ DB2-MYSQL2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑ DB3-MYSQL2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑ DB6-POSTGRESQL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>☑ DB7-MYSQL2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When you are done selecting the correct computer objects you can right-click anywhere in the right pane and choose **Go** from the menu. Only computer objects that are selected will be updated.

![Warning](image)

Enabling this option is required in order to move or delete multiple computers at once from the remote update dialog.
You can also clear / check all computers by right-clicking and choosing either **Clear All** or **Select All** from the menu.

The checkbox selection will be preserved when you perform actions/updates on the same group.

For example, if you want to install & start the EventSentry service on selected computers then you can do that. Your selection will be preserved as long as you right-click the same group in the left pane.

**Prompt for IP address when adding individual computers**

You can create easy to remember aliases for IP address in the management application when adding computers. By default you are only able to add host names to the computers container in a group, but when activating this feature you can optionally also enter an IP address.

**Auto-Refresh Active Directory Enabled groups upon startup**

If this option is checked and you have groups that are linked to Active Directory, then the management console will refresh each AD-enabled group with AD each time you open the management console. If this option is not checked then you will have to perform a remote update action (e.g. Check Agent Status) to refresh the list of computers.

**Authentication Method Preference**

When using alternate credentials for groups or computers, the management console can authenticate either by using Impersonation or by connecting to the remote IPC$ share. Impersonation is preferable, but not always supported. Adjust this option if you are having problems authenticating with remote computers.
Sort computer list
Checking this box will automatically sort the list of computers in the remote update window.

Minimize Network Traffic
If you are managing hosts that are spread across multiple sites over slow network connections, then it is recommended that you check this option. By default, EventSentry tries to determine what type of host the remote computer is running and also retrieves the current service status from the remote host when updating the configuration on remote hosts. Both features require additional network traffic and result in a slower update, and enabling this option will significantly decrease the time it takes to push the configuration to a remote host.

This option only affects the Update Configuration task, all other remote update options are not affected by this setting. You can always check the remote service status, including the version, by performing the Check Agent Status action.

Ping host(s) before attempting an update
Activating this option will ping a remote host before attempting any remote update action. If this option is checked and a remote host is unpingable, then EventSentry will not attempt a remote update and skip that computer.

Verify that service is running after an installation or update
When installing or updating a remote agent, remote update starts the service on the remote computer. Check this box to instruct remote update to wait for the service to successfully start. Clear the box to speed up the installation / upgrade of remote agents.

Verify that service is stopped after sending a stop request
When stopping the EventSentry service on remote computers, remote update can verify that the service has in fact stopped successfully. Clear this box to have remote update simply send the stop request without verifying that the service was stopped successfully.
Automatically push configuration when updating remote agents
Selecting this option will also push the current configuration out to the remote host(s) when performing an update of the remote agent (Manage Agent(s) -> Update).

Remote Share Preference
By default, EventSentry sends configuration updates to remote agents using the ADMIN$ share, though you may also setup the ES$ share if the ADMIN$ share is not available or cannot be used. As such, if you are using the ES$ share then it is recommended that you set this option to ES$ to speed up configuration updates.

3.1.5 Features
You can hide certain feature-containers in the tree pane if you are not using all features of EventSentry. This can make it easier to navigate in the management console since fewer containers are present in the tree pane.

Simply clear the check boxes of the features you wish to hide and they will not show up in the tree pane when you restart the management console.

You can also press the F5 key in the tree pane or right-click the computer container and select Refresh to immediately refresh the tree and show/hide the selected features.

3.1.6 Web Reports & Proxy
Path To Web Reports
If you have setup the web reports then it is recommended to specify the path here. Once configured you can view the web interface in your default web browser by selecting On The Web -> View Web Reports. Setting this option is also required for viewing a database-based heartbeat status inside the EventSentry GUI.

This setting is also necessary when using the heartbeat feature in connection with a database, so that the correct web pages are automatically displayed in management application.
Custom Search URL
You can use the built-in event viewer to query the following web sites for details on an event log entry:

5. A custom search page

Options 1 - 4 cannot be changed, however you can enter your own search page to the Custom Search URL field. You can use the variables $EVENTID and $EVENTSOURCE in the URL.

Proxy Settings
The news and feedback features of the management console all work through the HTTP protocol. If your network requires a proxy server then you can specify the proxy server and port here.

If you are using Internet Explorer then you can simply check the "Use Internet Explorer Settings" checkbox to instruct EventSentry to automatically use the proxy settings configured in Internet Explorer.

3.1.7 QuickTools

The QuickTools allow you to execute command utilities from within the management console. They are integrated into the computer groups, and allow you to run any application against a remote computer with the click of a button. You can configure up to eight QuickTools, and each tool can utilize the same credentials that are setup for remote update (if they have been configured for a computer or group). The following options are available for each entry:

Name
Specify a descriptive name for the tool. This name will be shown when you right-click a computer item.

Command Line
Specify the command line for the tool. Use the $COMPUTER variable, which will automatically be replaced with the name of the selected computer.

Prompt
For potentially disruptive tools, such as a reboot, EventSentry can prompt you before it will execute the tool.

Authenticate
Check this box if EventSentry should authenticate before executing the tool. Credentials are taken from the group or computer, if configured.
Hide
Checking this box will hide any Windows opened by the command directly executed by the management console; it will not prevent any subsequent windows from appearing. This can be useful to hide a command line windows for example.

To access the QuickTools, simply right-click any computer in a computer group and select the QuickTools submenu:
3.2 Event Log Viewer

The EventSentry GUI includes a self-adjusting, built-in event log viewer that lets you perform basic event log functions from within EventSentry. In most cases, you will not have to open another event log viewer application. You can also view up to 15 remote event logs, please see Viewing Remote Event Logs for more details.
Automatically include or exclude events just by right-clicking them

Instead of setting up include or exclude filters manually, you can simply locate them in the **local or a remote event log**, right-click them and select either "Add Include Filter" or "Add Exclude Filter". This will show the following dialog.
where you can specify a name for the new event log filter and select a package where you would like the filter to be created.

Alternatively you can also click the include and exclude buttons on the event log detail dialog:
Easily Filter Events
You can easily filter out events based on the event severity. Simply right-click anywhere and select the severity you would like to see:
For example, to see only warnings select "Warning". To see both errors and warnings, simply select "Error" in addition to Warning.

To disable the filter again, select "All Records". While this feature is not as flexible as the filtering mechanism of the event viewer that ships with the operating system, it does make basic filtering much easier to use.

**View multiple event logs at the same time**
You can view the event logs of (up to 15) remote machines (more info)

**View Time Span**
You can immediately see how many event log entries are present and the amount of time an event log spans

```
System: 19434 event(s) spanning 327 days, 15 hours and 52 minutes
```

**Event log summary information in the status bar**

**Automatic Column Hiding**
If the Category or User column is empty then it is automatically hidden.

**Frequency**
View the frequency of an event log record (how often a similar event record appears in the event log). This statistic is initially calculated for the first 3000 (or less if fewer records are present) event records and then dynamically calculated as you scroll through the event log.
If you would like to see accurate statistics then you can right-click on any event log record and select **Load All Records** from the menu.
The event record shown above occurred 1806 times in the current event log. The frequency is calculated by taking the event id and the event source into consideration.

Sometimes event records can contain unique insertion strings despite a unique event id. In this case the frequency will not be 100% accurate.

Automatic Submission of Comments
You can quickly and easily submit comments regarding an event log record to the myeventlog.com web site. Simply enter a comment in the “Advanced” field and click the “Submit” button:

Query web sites for more information on event IDs
You can query the following web sites from the EventSentry Event Log Details dialog to obtain additional information on an event log entry:

1. MyEventlog.com (http://www.myeventlog.com/)
2. Google (http://www.google.com/)
3. Microsoft Knowledge Base (http://support.microsoft.com/)
4. Microsoft.com (http://www.microsoft.com/)
5. A custom search page

Column Sorting
Output can be sorted by clicking on the respective column header.
3.2.1 Viewing Remote Event Logs

Up to 15 remote event logs can be viewed from the management application. You can choose the remote computer in three ways:

1. Manually specifying a remote computer
   Right-click the “Event Log Viewer (local)” object and select “Connect ...”. You will be prompted to enter a remote computer name.

2. Choosing a computer from a group
   Right-click the “Event Log Viewer (local)” object and select a group name and computer name from the menu.

3. Previously selected computer
   EventSentry caches up to the last 3 computers you successfully connected to recently. Right-click the “Event Log Viewer (local)” object and select on of these 3 (or less) computers.

Including / Excluding events from remote computers
When you include or exclude events by right-clicking event log records, they will automatically show up in the group where that computer is located in. For example, when you connect to the computer CHEETAH which is located in group FILESERVERS and exclude any particular event, then the resulting filter will be created in the FILESERVERS group.

Disconnecting
To disconnect from a remote event log, simply right-click the computer's event log object and select Disconnect. When you exit the application all remote event logs will be closed automatically. Note that connections to remote event logs will not be automatically restored upon restarting the management application.

3.2.2 Viewing Event Log Backup (.evt) Files

Starting with version 2.70 of EventSentry you have the ability to open event log backup files. Event Log backup files are usually created with the Windows event viewer, the EventSentry event log backup feature or with other event log management applications.

To open an .evtx file, right-click the “Event Log Viewer (local)” container and select ”Open Log File ...”. You will then be prompted to browse for an .evtx file to open.

Avoiding a prompt for the event log
In order to display a previously saved event log properly, an event log management application needs to know from which event log it was originally exported:

You can avoid being prompted for the event log by making sure that the filename contains either the full name or an abbreviation of the event log it was exported from. EventSentry will recognize the following names and abbreviations:
Full name of event log | Abbreviation
---|---
Application | app
Security | sec
System | sys
DNS Server | dns
File Replication Service | rep
Directory Service | dir

For example, if the file name is `fileserver_app_01122005.evtx` then EventSentry will automatically associate this file with the Application event log.

EventSentry does not automatically recognize custom event logs. As such, if you are opening an .evtx file that was exported from a custom event log then you will either have to select the custom event log from the drop-down menu or specify the name manually.

**Double-Clicking .evtx files in explorer**
You can configure EventSentry to be the default handler for .evtx files. With this feature enabled you can double-click .evtx files in Windows explorer, which will automatically display the .evtx file in the EventSentry management console. See options for more information.

### 3.3 Utilities

#### 3.3.1 Agent Database Status Utility

The agent database status utility, `es_db_agent_status.exe`, queries the database to detect an extended period of database inactivity from one or more agents. Running this utility ensures that all agents are online and reporting data in the database.

The utility can either be run on-demand from the command line, or be scheduled on a regular basis using a scheduling engine like the EventSentry application scheduler or the Windows Task Scheduler. The agent database status can also be reviewed on-demand through the "Agent Status" page in the maintenance menu of the web reports.

Using command line arguments, the utility can either inspect data from all features an agent is using, or can only query for specified features - e.g. Event Logs only.

**Required Options**

- `<SYSTEM DSN>`
  A System DSN pointing to the EventSentry database or, if an EventSentry agent is installed on the same machine where you are running the utility then you can specify the name of the EventSentry action instead of the DSN name.
- `<ACTION>`
  The feature to verify, or **AllTables** to evaluate all features an agent is currently monitoring.
- `<MINUTES>`
  The maximum period of database inactivity, in minutes. If the most recent database entry from a host is older than `<MINUTES>`, the host will be listed as inactive.
- `<USER>`
  Specify a user that has permissions to query (SELECT) data, usually `eventsentry_web`.
- `<PASS>`
  Password of `<USER>`

**Optional Options**

- `/V`
  Verbose output, useful when utilizing "AllTables" feature

---

On Windows Vista and later, the purge utility needs to be executed from an elevated command prompt ("Run as Administrator") if it references an EventSentry action.
Examples

1. Connect to the “Primary Database” action and verify that all hosts reported event log data in the last 30 minutes:
   es_db_agent_status "Primary Database" EventLog 30 eventsentry_web 4h3Passw0rd

2. Connect to the MyDSN system DSN and verify that all hosts reported performance in the last 15 minutes:
   es_db_agent_status MyDSN Performance 15 eventsentry_web #df2er

3. Connect to the MSSQL action and verify that all hosts reported data for all configured features in the last 60 minutes:
   es_db_agent_status MSSQL AllTables 60 dbreader MyP4ssw0rd!

4. Connect to the MySQL action and verify that all hosts reported Event Log, Syslog & SNMP Trap data in the last 3 hours:
   es_db_agent_status MySQL EventLog,Syslog,Snmp 180 eventsentry_web thePa55w0rt

5. Connect to the “Primary Database” action and verify that all hosts reported Event Log and Logon Tracking data within the last 24 hours:
   es_db_agent_status "Primary Database" EventLog,LogonTracking 1440 eventsentry_web datpa55w00rd

3.3.2 Configuration Assistant

The configuration assistant usually launches after the initial setup and after major version upgrades where it updates the database schema and configures new components. The configuration assistant is also used to initialize any new databases.

- Configure a new SMTP action if no SMTP action is current setup
- Update all databases which are referenced through an action to the latest schema
- Setup a new database, including action, if no database actions are currently configured
- Setup and configure an individual database if launched from a database action dialog in the management console
- Install & configure the heartbeat agent
- Install & configure the network services
- Install & configure the ADMonitor component

The configuration assistant is automatically launched after every installation / upgrade.

Prerequisites

The configuration assistant resides in the config_assistant sub directory and requires the following files to run:

- es_config_assistant.exe
- Qt5Core.dll
- Qt5Gui.dll
- Qt5Xml.dll
- Qt5Widgets.dll
- msvcp140.dll
- concrt140.dll
- vccorlib140.dll
Command-Line Parameters
The utility supports a single command line parameter, "/initdb", which needs to be followed by the name of a database action. For example:

```
es_config_assistant.exe /initdb "Primary Database"
```

This will either initialize the database pointed to by the “Primary Database” action, or update the existing database to the latest schema.

3.3.3 Database Purge Utility
The database purge utility is installed as part of the Web Reports feature, and can be found in the “Database Wizards” sub folder of the EventSentry installation folder.

Required Options

A System DSN pointing to the EventSentry database

Required Options

A System DSN pointing to the EventSentry database or,

- `<SYSTEM DSN>`
- `<ACTION>`
- `<FEATURE>`
- `<DAYS/HOURS>`
- `<USER>`
- `<PASS>`

Optional Options

- `/count`
- `/test`
- `/shrinkdb`
- `/shrinklog`
- `/shrinkindexes`
- `/log:<FILENAME>`
- `/utc`

Examples

1. Purge all data from the “Primary Database” older than 90 days

```
es_db_purge.exe "Primary Database" All Tables 90d postgres postgrespw
```

2. Purge all event log data from the “Archive Database” action which is older than 366 days

```
es_db_purge.exe "Archive Database" Event Log 366d postgres postgrespw
```
3. Determine how much Syslog data is **older than 30 days**

```
es_db_purge. exe "Primary Database" Syslog 30d /test postgres postgres
```

**Schedule**

We recommend that you schedule the utility, for example through the EventSentry application scheduler (or the Windows task scheduler), to run on a regular basis **at least** every month. This ensures that your database does not accumulate unnecessary data.

The following table explains all supported feature names. You can also use the **AllTables** keyword to purge data from all tables.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventLog</td>
<td>Event log records</td>
</tr>
<tr>
<td>Diskspace</td>
<td>Disk space data</td>
</tr>
<tr>
<td>Performance</td>
<td>Performance data</td>
</tr>
<tr>
<td>ProcessTracking</td>
<td>Compliance: Process tracking data</td>
</tr>
<tr>
<td>LogonTracking</td>
<td>Compliance: Console Logon tracking data</td>
</tr>
<tr>
<td>PrintTracking</td>
<td>Compliance: Print tracking data</td>
</tr>
<tr>
<td>HeartbeatHistory</td>
<td>Heartbeat history</td>
</tr>
<tr>
<td>HeartbeatPing</td>
<td>Heartbeat ping history</td>
</tr>
<tr>
<td>ServiceHistory</td>
<td>Service history</td>
</tr>
<tr>
<td>SoftwareHistory</td>
<td>Software history</td>
</tr>
<tr>
<td>EnviroTempHumid</td>
<td>Temperature and humidity (if available) data</td>
</tr>
<tr>
<td>EnviroMotion</td>
<td>Motion data</td>
</tr>
<tr>
<td>Nessus</td>
<td>Nessus data</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog data</td>
</tr>
<tr>
<td>Snmp</td>
<td>Snmp data</td>
</tr>
<tr>
<td>FileMonitoring</td>
<td>File Change monitoring data</td>
</tr>
<tr>
<td>LogFileDelimited</td>
<td>Data from delimited log files</td>
</tr>
<tr>
<td>LogFileNondelimited</td>
<td>Data from non-delimited log files</td>
</tr>
<tr>
<td>FileAccess</td>
<td>File Access Tracking data</td>
</tr>
<tr>
<td>RegistryTracking</td>
<td>Registry tracking data</td>
</tr>
<tr>
<td>UptimeHistory</td>
<td>Uptime history</td>
</tr>
<tr>
<td>ActionHistory</td>
<td>Action trigger history</td>
</tr>
<tr>
<td>ReportHistory</td>
<td>Report history</td>
</tr>
<tr>
<td>AccountMgmtUser</td>
<td>Compliance: Account Management Tracking (Users)</td>
</tr>
<tr>
<td>AccountMgmtGroup</td>
<td>Compliance: Account Management Tracking (Groups)</td>
</tr>
<tr>
<td>AccountMgmtComputer</td>
<td>Compliance: Account Management Tracking (Computer)</td>
</tr>
<tr>
<td>LogonAuthFailure</td>
<td>Compliance: Network Logon (Failure)</td>
</tr>
<tr>
<td>LogonAccountAuth</td>
<td>Compliance: Network Logon (Domain Account Authentication)</td>
</tr>
<tr>
<td>LogonByType</td>
<td>Compliance: Network Logon (Logon By Type)</td>
</tr>
<tr>
<td>PolicyChange</td>
<td>Compliance: Policy Change Tracking</td>
</tr>
<tr>
<td>LargeFiles</td>
<td>Disk Space data (large files only)</td>
</tr>
<tr>
<td>ScheduledTasks</td>
<td>Scheduled Tasks inventory data</td>
</tr>
<tr>
<td>NetFlow</td>
<td>NetFlow data</td>
</tr>
<tr>
<td>ADMonitor</td>
<td>ADMonitor object changes</td>
</tr>
<tr>
<td>ADMonitorGroupPolicy</td>
<td>ADMonitor group policy changes</td>
</tr>
<tr>
<td>SysmonNetwork</td>
<td>Sysmon network data</td>
</tr>
</tbody>
</table>
3.3.4 Log Import Utility

Using the EventSentry Log Import Utility, you can import previously backed up event log files (.evtx) or log files (e.g. IIS, DHCP, etc.) into a EventSentry database so that they are search-able in the web-based reports.

Benefits

The EventSentry Log Import Utility is useful for administrators who backup all their event logs automatically with EventSentry on a regular basis but with limited database storage. Using the utility, the backed up .evtx files can be imported into the database anytime. You can also use the utility to import EVTX files have been backed before you started using EventSentry.

You can also use the utility to import delimited and non-delimited log files into the EventSentry database. Since the utility supports command-line parameters and can run silently, it is particularly useful for importing log files on a scheduled basis.

![EventSentry Database Import Utility](image)

Start the utility on a computer where you installed EventSentry with the setup application, including the management console component. You can then either start the utility through the start menu (Start ->...
Management Console / Utilities

Programs -> EventSentry -> EventSentry Database Import Utility) or by selecting "Tools -> Utilities -> Database Import Utility".

If you are importing an event log back file then you can also right-click the "Event Log Viewer (Local)" container in the management console and select "Import Log File to Database".

Importing Event Log Backup Files
Select the event log backup (.evtx) file and select the type of event log the file contains. If the file name contains either the strings "app", "sec", "sys", "dns", "rep" or "dir", then EventSentry will automatically detect the event log and pre-select the event log. Making sure that the event log selection is correct is important, so that the database import utility knows how to translate event log IDs into real messages.

Limitations
If the total number of EventSentry licenses you purchased is less than 10, then the computer from where you are importing the event log backup file, needs to be present in an EventSentry group. If the computer is not present, then you will need to add the computer to a group using the management console and restart the utility.

Importing Delimited and Non-Delimited Log Files
Select a delimited or non-delimited log file to import. If you are importing a delimited log file then a log file definition will need to exist in order to correctly import the file. If no definition exists then you will need to close the utility and create a log file definition first.

The database import utility will automatically update the "Number of lines" and "File Size" values in the "Import Progress" section after a file was selected with the "Browse" button. The utility will also detect automatically if a file contains a Unix line separator and import those files correctly as well.

Destination
Select the database notification action that you wish to write the data to. If your EventSentry installation contains only one database notification action, then it will automatically be selected and the pull-down menu will be grayed out.

Import Progress
Once you have verified that your selection is correct you can click the "Start Import" button to start the import. This area also shows you the size of the event log backup file you are about to import, and the number of event log records contained in the event log backup file.

The progress bar will show you how much data has been imported so far and you can abort the import anytime.

Command-Line Options
The EventSentry Database Import Utility supports the following command-line options:

<table>
<thead>
<tr>
<th>Command-Line Option</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>/file:</td>
<td>The event log backup (.evtx) or log file to import</td>
<td>/file:server01_app_072006.evtx</td>
</tr>
<tr>
<td>/action:</td>
<td>The name of the EventSentry action to write the data to</td>
<td>/action:mssql</td>
</tr>
<tr>
<td>/eventlog:</td>
<td>The name of the event log contained in the event log backup file</td>
<td>/eventlog:Security</td>
</tr>
<tr>
<td>/filedefinition:</td>
<td>Name of an EventSentry log file definition</td>
<td>/filedefinition:IIS</td>
</tr>
<tr>
<td>/nondelimited</td>
<td>Indicate that the file to import is a non-delimited log file</td>
<td></td>
</tr>
<tr>
<td>/unix</td>
<td>Force utility to use a Unix line terminator</td>
<td></td>
</tr>
</tbody>
</table>
/debug Enable debug logging to %SYSTEMROOT% \system32\eventsentry /debug

/? shows supported command-line options /?

For example, to automatically record the security event log from file DBSRV01_SEC-062006.evtx to the Primary Database action, execute the following command:

eventsentry_db_import.exe /file:"c:\logs\DBSRV01_SEC-062006.evtx" /eventlog:Security /action:"Primary Database"

If you need to import multiple log files into the mssql action, then you can create a batch file, for example:


To import an IIS log file, which is a delimited log file, into the database, execute the following command:

eventsentry_db_import.exe /file:ex070828.log /filedefinition:"IIS 6" /action:mssql

3.3.5 Event Message Browser

The built-in event message browser lets you view all available event messages that may be logged on your system. You can simply select an event log (e.g. Application) and select one of the available event sources from that log (e.g. ntbackup) and then review all the available Event IDs from that source.

General

When launched from the filter dialog, the event message browser lets you apply the basic event properties to the filter. Additionally, you can also generate the selected event in the event log by clicking the Test button.

The event message browser can be launched from the filter dialog by clicking the Lookup button, or through menu at Tools -> Utilities -> Event Message Browser.

Insertion Strings / Creating Test Events

Most event messages use so-called insertion strings, indicated by the percentage sign followed by a number. For example, an event message in the event message browser might include the string %1, which will be replaced with useful data at run-time. For example, the event message (event id 10100 from EventSentry):

The status for service %1 (%2) changed from %3 to %4.

will look similar to the one below when logged to the event log:

The status for service Winmgmt (Windows Management Instrumentation) changed from Running to Stopped.

since EventSentry will replace the insertion strings %1, %2, %3 and %4 with data that is relevant to the current operation. When creating a test event through the event message browser, the insertion
strings will all be replaced with the text specified in the Test String field, which is EventSentryTest by default.

You cannot create test events from the events in the Security event log with the event message browser at this time.

The screenshot below shows the event message browser with the above event being displayed:

3.3.6 Protocol Parser (Collector)

The protocol parser can examine dump files generated by the EventSentry collector or the temp file generated by agent for troubleshooting purposes. Running the protocol parser utility should only be necessary under the following circumstances:

1. The collector logged event 142 or 143
2. The temporary file generated by the agent while a collector is offline and needs to be examined

The protocol parser utility (protocol_parser.exe) is located in the "resources" sub directory of the EventSentry installation directory.

Collector event 142 & 143

When the collector is unable to successfully parse a packet it will log event 142 and/or 143 and dump the packet contents to a file ending with the .dump extension in the %SYSTEMROOT%\system32\eventsentry\temp\collector directory. Simply pass the file name as a parameter to the protocol parser utility.

Agent Collector Backup File

The agent will log all cached data the %SYSTEMROOT%\SysWOW64\eventsentry\temp\eventsentry_collector.client_backup.tmp file when a collector is unavailable if the cached data cannot be stored in memory or if the agent is stopped. Simply pass the file name as a parameter to the protocol parser utility.
3.3.7 Remote Update Utility

See "Automating Remote Update" for more information on the remote update utility eventsentry_upd.exe.

3.4 Exporting, Importing and Saving the Configuration

The entire EventSentry configuration is stored in the registry and can be easily exported / imported. This might be useful when you have multiple installations of EventSentry behind a firewall. Exporting the configuration on a regular basis is highly recommended for backup purposes. Alternatively you can also save the configuration as a HTML file for documentation purposes.

Exporting

To export the configuration into a .reg registry file either right-click the computer object and choose Export Configuration

or choose Export from the Home tab.

Importing

To import the configuration to a target computer you will first have to transfer the previously created .reg file to the target computer. You can then either

- Open the EventSentry GUI and, as described under Exporting above, either right-click the computer object and select Import Configuration or choose Import from the File menu. The GUI will be closed for the change to take effect.

- Double-click the .reg file in explorer to import it into the registry. Please note that the GUI (eventsentry_gui.exe) has to be closed when you import the configuration as the imported settings might otherwise be overwritten by the GUI.

Saving the Configuration

To save the entire EventSentry configuration in a HTML file, select “Save as Html” option the Home tab. All configuration options, with the exception of GUI settings from the Tools -> Options dialogs, will then be written to the specified file which can be opened in any major web browser such as Internet Explorer,
Firefox and Chrome. Please note that you cannot import the configuration from a .html file at a later time, this can only be accomplished if you export the configuration (see above).

3.5 Checking for New Versions

In addition to checking for the latest version of EventSentry on the product web site, you can also use the management console to easily determine if you are running the latest version of EventSentry and download any applicable patches.

To check for a new version or patch, navigate to the Help -> Check for Updates which will show a dialog similar to the one shown below:

The Version Information dialog shows you the three major components of EventSentry and whether they are up to date or not. If the “Current” column shows “Yes” and a green checkbox is shown next to the component, then it is up to date and no action is needed.

The update feature will detect the following:

- Patch availability: You are running the latest version, but a patch that addresses specific issues has been released
- New version available: You are not running the latest version
- Up-To-Date: You are running the latest version

**Patch Availability**

If a patch for EventSentry has been released, then you can use this feature to automatically download and install the patch. The dialog below shows an installation that is running version 3.0.0.16, however the latest version 3.0.0.25 is available (which also includes a critical fix). As a result, the Recommended Action is to download and install the latest patch to bring the installation up to date.

If you opted into the online maintenance expiration check and have an active maintenance agreement or an active trial, then the latest installer can be downloaded directly through the management console. The online maintenance check can be enabled under Tools -> Options -> Version Check / Welcome -> “Enable online maintenance expiration check and integrated patch download”. If you have opted out of the online maintenance check or do not have an active maintenance agreement, then you can download the latest installer from the customer area.

Click the Download & Install Patch button to begin the download of the patch. Downloaded installers will be stored in the Patches sub directory of your EventSentry installation, for example C:\Program Files\EventSentry\Patches.
New Version Availability

If a new version for EventSentry has been released, then the Recommended Action will indicate that you can download and install a new version and a Download button will be displayed. Since downloading a new version requires a current maintenance agreement, clicking the download button will take you to our software update page that requires you to login in with your registered email address and password.

Please see the sub-chapters of Updating to a new version for more information about updating to the latest version.

Automatically Checking for new Versions

In addition to invoking the Check for Updates feature through the help menu, you can also configure EventSentry to automatically check for new versions and patches every time the management console is launched.

You can configure this feature by navigating to Tools -> Options -> Version Check / Welcome, more information can be found here.

3.6 Testing Event Log Filter Rules

The Filter Rules Test utility allows you to test your filter rules against actual event log events, without having to actually wait for events to happen. The utility is also integrated with the built-in event log viewer, and will show you which filter rules would match the event, including the action that would be triggered.

This makes it easy to ensure that your event log filter rules are setup correctly.
Launching the Filter Rules Test Utility

You can either launch the utility through the main menu by navigating to **Tools -> Utilities -> Filter Rules Test Utility**, or you can access the tool by right-clicking an event from the built-in event log viewer and selecting “Test against filter rules”. The latter is generally easier, as all the event properties are automatically filled into the “Event Log Record” section.

**Computer**

Since event log filters are assigned to computers and groups, different computers might have different rules assigned to them. As such, EventSentry needs to know which filter rules to load and test against. If you do not specify a computer name here, then the event log record will be tested against all filter rules.

**Verbose:** Show all filters, including non-matching
Checking this option allows you see exactly why a filter is not matching your event. By default, the tool will only display the first filter rule that matches the event specified in the "Event Log Record" section. This means that if an event matches an exclude and an include filter for example, then only the exclude filter will be shown without the "Verbose" option.

Filters that do not match the event will not be displayed. For example, if you need to troubleshoot why a filter you created isn't matching and processing a given event, then this option will show you all non-matching filter and indicate why it didn't match the event.

**Event Log Record**
Specify as many properties from the actual event as possible. You are required to enter at least the:
- Event Log
- Event Severity
- Event Source
- Event ID

**Viewing the Results**
Click the TEST button to view the results of the test. The results will look similar to the screenshot shown below if you do not check the "Verbose" check box:

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Package</th>
<th>Match Reason</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Critical Events</td>
<td>Email Notification</td>
<td>Default Email</td>
<td></td>
</tr>
<tr>
<td>Consolidate Non-Security...</td>
<td>Database Consolidation</td>
<td>Primary Datab...</td>
<td></td>
</tr>
</tbody>
</table>

Note that the "Match Reason" will be empty if the matching filter does not have a source, category, event id or event detail configured. Otherwise the column will show which fields of the filter matched the event.

If you select the "Verbose" option, then the output will look slightly different and include additional columns:
The list will now include all filters, and non-matching filters will indicate why they did not match the event that was passed. For example, most of the exclude filters in the above screenshot did not match the event because the severity selected in the filter did not match the event severity.

You can double-click a filter in the list to locate and edit the filter details.

### 3.7 Wizards

Starting with EventSentry 2.72, the management console now includes wizard to help new users accomplish common tasks more easily, and to help understand the concept of EventSentry more quickly.

The wizards can be accessed through the **Wizards** menu option and the following wizards are currently available.

**Event Log Filter Setup**

This wizard will guide you through the creation of a basic filter, and also supports the following advanced properties:

- Day/Time Restrictions
- Summary Filter
- Recurring Event Filter
Since the Event Log Filter Setup Wizard is intended to be used mostly by new users, advanced filter options such as thresholds, timers and custom event logs are not supported by the Event Log Filter Setup Wizard and will have to be configured directly at the filter.

**Database Consolidation**

The Database Consolidation Wizard will guide you through the process of setting up database consolidation, if it was not setup through the installation process. This wizard will create an action (it will however not initialize the database, but give instructions), allow you to specify the types of events you plan on consolidating, and give you the option of collecting system health and/or tracking data to the database.

More wizards are planned in the future, and you are encouraged to email us suggestions for new wizards. Please also check out our tutorials at [http://www.eventsentry.com](http://www.eventsentry.com) -> Support.

### 3.8 Toolbar (Legacy)

The legacy toolbar is either displayed when the ribbon is disabled (Tools -> Options -> General) or when the management console is running on a machine with Windows XP or Windows 2003. The toolbar allows you to do perform various actions quickly with the click of button, instead of having to right-click containers or navigate through the menu.
Brings you to the home screen
Rebuilds (refreshes) the tree in the left pane
Saves the configuration
Cuts the current selection, only valid with computer, filter and action items
Copies the current selection, only valid with filter and action items
Pastes the previously copied/cut item
Allows you to search for filters or computers
Downloads the latest packages from www.eventsentry.com
Pushes the latest configuration to all computers in all groups
Starts the remote update if "Use Checkboxes" is configured
Views the web reports if configured
Opens http://www.eventsentry.com in your default browser
Opens the EventSentry Welcome Wizard
Navigates to the EventSentry knowledge base
Opens this help file

3.9 Searching

It is sometimes difficult to know whether a filter for a particular event already exists, or to find out which group a computer belongs to.

The Find Dialog allows you to search for filters and computer in an easy way. You can reach the find dialog in three ways:

- Pressing CTRL+F
- Selecting Find from the Edit menu
- Pressing the find button on the toolbar

Once the Find dialog has been displayed either select the Filter or Computer tab.

Filters
Select this tab to look for filters with certain properties, for example you can display all filters with the event source set to "NETLOGON". You can also display all filters assigned to a particular computer or group. See Searching for Filters for more information.
Computer
Select this tab to locate a computer in your configured groups. Simply enter the computer name in the Computer field and click Find. The computer will be selected in the tree if it exists.

3.9.1 Searching for Filters
When you have a large number of packages and filters then it can be difficult to locate a filter among all packages. The Find feature allows you to search for filters based on most event properties of a filter, including:

- Log
- Source
- Category
- ID
- Username
- Computer
- Filter Name
- Description

You can also search for filters based on general properties:

- assigned actions
- filter type (include or exclude)
- filters with thresholds
- filters with schedules
- filters with timers

Finally, you can only display filters that are assigned to a particular computer or group:

After you have selected the filter properties and clicked the Find button, a list of filters matching your search criteria will be displayed, showing you the most common properties of a filter:
To view all filter details, simply double-click a filter from the list which will locate the filter in the left tree pane and show the filter details in the right pane.
4 Working with EventSentry

4.1 Welcome Screen

The Welcome Screen is displayed in the Details Pane after you started the EventSentry management console. To view the welcome screen manually click on the root computer item.

![Welcome Screen Screenshot]

Visit our new site with access to all Windows Security Event IDs - including GeoIP lookups

- **Agent** Running v3.6.0.14 x64
- **Collector** Running v3.6.0.14 x64
- **Heartbeat Monitor** Running v3.6.0.14 x64
- **Network Services** Running v3.6.0.14 x64

**Step 1:** Add hosts to EventSentry (import or link from AD or files, network discovery, manually)

**Step 2:** Deploy agent to remote hosts

**Step 3:** Access Web Reports

Maintenance agreement is valid until Mon 1/27/2020

**Header**

The top right of the orange header shows the version of the management console as well as the configuration revision. The configuration is simply an incremental number that is incremented by one every time the configuration is saved.

**News**

Shows the latest news update about EventSentry, clicking the link will open a web browser and navigate to the corresponding web page.

**Service Statuses**

The green tiles below the latest news show the status of all installed services, including their version. Unless a custom binary was issued by support, all components should run the same version, as shown above.

**Steps**

Shows the recommended steps to take after installing EventSentry.

**Maintenance Agreement**

Shows the current status of the maintenance agreement if you are running the full version of EventSentry.

All tiles are clickable (with the exception of the top orange tile)
4.2 Collector

The EventSentry Collector, introduced in version 3.2, enables a 3-tier architecture between an action (e.g. database, email server) and the EventSentry agents. When enabled, the collector will provide functionality similar to a proxy server (although with significantly more functionality), and communicate with a support EventSentry action on behalf of a remote agent. The collector supports compression as well as secure TLS encryption.

The collector can be enabled during the installation (default behavior), or configured after an installation or upgrade. An action will be routed through a collector under the following circumstances:

- A collector is configured (and running) in the "Collector" settings
- The action can be routed through a collector (see "Supported Actions") and configured to use a collector

It is possible and supported to only route some actions through a collector but configure other actions for direct agent-to-action communication.

Supported Platforms
The collector is available as a 64-bit (x64) and 32-bit (x86) binary. The 64-bit binary is recommended and installed by default on 64-bit Operating Systems.

Supported Actions
The following actions can routed through a collector:

- Database
- Email (SMTP)
- Syslog
- File

All other actions either communicate directly with the remote action (e.g. HTTP action) or execute locally (e.g. process action).

Supported Components
The following components can currently utilize the collector, all other components still communicate directly with their respective actions:

- Agents
- Heartbeat Service
- Network Services

Advantages
Utilizing the collector has the following benefits:

1. Communication between the agents and the collector can be encrypted for increased privacy, useful for hosts transmitting data over an insecure network (e.g. laptops)
2. Communication between the agents and the collector can be compressed to reduce bandwidth consumption
3. Security can be increased by restricting actions, such as a database or email server, to only allow access by the collector instead of all agents
4. Database: All data is cached by the agent when the collector is temporarily unavailable. Only event log data is cached when not using a collector while the database is unavailable
5. Database: Although automatically managed by the EventSentry agents, ODBC drivers do not need to be installed on the agents
6. Database: The database login credentials do not need to be transmitted to the agents since they are not directly connecting to the database.

7. Agent Management: The collector can automatically transmit configuration and agent updates to remote agents.

Disadvantages
In some cases the traditional method where agents communicate directly with an action may be preferable. The collector provides little benefit in the following scenarios:

1. The entire installation only spans a single host.
2. The agents have a direct connection with the database or email server.
3. Data sent from the agent to the action is already transmitted over a secure network.
4. Data sent from the agent to the action is already transmitted over a fast network where compression provides little or no benefit.
5. The action (e.g. database) is reliable and has little or no downtime.
6. Installing and/or maintaining one or more collectors is not desirable.

Redundancy
Since the collector is potential single point of failure (SPOF), EventSentry offers the following features to ensure maximum availability:

- Agent store all data in a persistent local cache if they cannot reach the collector. Data is resubmitted as soon as the collector is reachable.

- The collector caches all data if it cannot reach an action (e.g. database, email server) in memory and is flushed to disk when the collector service is stopped. Cached data is paged to temp files if the in-memory cache (aka queue) exceeds either a hard limit or is unusually high based on previous usage.

  The collector logs event id 210 when paging starts followed by event 214 when paging is disabled. The collector requires at least 500Mb of free disk space on the %SYSTEMROOT% drive in order to support disk paging.

- Multiple collectors can be configured for additional redundancy.

Performance
The collector service is designed to support both a large number of clients as well as large amounts of data in real time. For database actions, the collector uses multiple (~20) concurrent db connections to ensure a high throughput. The current status of the collector can be reviewed in the web reports under the Tools/Maintenance menu section ("Collector Status") if "Collect statistics" is enabled.

4.2.1 Configuration
The collector is configured via the “Collector” button in the navigation tree and ribbon ("Home -> General") of the management console. The collector icon in the tree view is displayed in color when the collector service ("EventSentryCollector") is running, or displayed in gray when the collector is either not installed or not running.
Hostname
Specifies the host name to which the remote agents will connect to, this should either be a host name which can be resolved by all hosts or an IP address. If the collector should be contacted from both the internal LAN as well as remote clients which connect through a firewall, then split DNS can be configured.

Multiple collectors can be separated with a comma, see “Multiple Collectors” for more information.

Enable Compression
Compresses all data before it is transmitted to the collector, reducing the overall bandwidth consumption of the agent. The compression factor depends on the data collected and usually ranges between 15 and 25% (subsequently reducing the amount of data transmitted by about 20%). Enabling compression is recommended in most cases and enabled by default.

**Collect Statistics**
Collects the following basic performance statistics in the database, see [Collector Status](#) for more information.

**Enable Cleartext Communication**
Transmits all data, including log contents, via clear-text over the selected TCP port. Data is encoded but not encrypted. Cleartext communication is not recommended.

**Enable Encrypted Communication**
Transmits all collected data over a secure TLS channel. Encrypted communication is preferred when both clear-text and encryption are enabled.

**Deploy Configuration Updates**
Instead of manually pushing configuration updates from the management console with remote update, the collector can send configuration updates to all connected agents automatically. This is particularly useful for clients which are not permanently connected to the network where the management console, e.g. laptops.

- **Automatic**
  Any time the configuration is saved in the management console the collector will automatically deploy it to all connected remote agents.

- **Semi-Automatic**
  Only automatically distributes an updated configuration if the configuration is saved with the "Save and Deploy" option. Simply clicking the "Save" button will save the configuration locally, but not deploy it network-wide.

When a configuration update is approved, either manually or automatically, it may take several minutes before it is loaded by the remote agent.

Agents running on hosts where EventSentry was installed with the setup (usually affects only one host) will not accept remote configuration updates and instead load the configuration
Keep remote agents up to date
Instead of manually upgrading remote agents whenever a patch or version update are installed, the collector can push an updated agent to all connected hosts. Once the remote agent receives an updated agent binary, it will update and restart itself automatically. This feature only works for agents running v3.3.x or later.

It may take up to 2 minutes before an agent update is sent by the collector, if a remote agent with an outdated agent is detected.

See Collector Security Configuration for more information.

4.2.1.1 Security
The collector is designed to allow for a secure and reliable data transmission between the EventSentry agents and the collector. Most security settings below only apply when TLS communication is enabled.

TLS Encryption
Certificates for TLS communication are created automatically by the collector when the service starts for the first time. Certificates are created with a bit length of 2048 bits (1024 bits on Windows Server 2003) using SHA256 as the signature algorithm.

Ciphers
The agent(s) and collector negotiate the most secure cipher available on both hosts. The cipher used depends on the Operating System as well the Schannel configuration on Windows (both on the client (agent) and the server (collector)).

It is recommended to run the collector on the newer version of Windows (2012 or higher) if possible, to ensure that the most secure ciphers are available.

Default Security Features
The following security features are always enabled, regardless of the security level selected below.

Shared Secrets
When an EventSentry agent connects to a collector for the first time, it generates a unique id as well as a shared secret (password) which it sends to the collector over an encrypted TLS channel. The collector then stores the shared secret locally and associates it with the remote host's unique id. Once the shared secret is associated with the remote host, only connection attempts which match the locally stored shared secret will be accepted. This ensures that a remote host can not be impersonated.

Certificate Validation (Agents)
When an agent connects to a collector for the first time, it downloads the remote host's certificate and caches it locally. Any future connection attempts to the same collector compare the certificate presented by the collector with the locally cached certificate. The connection is aborted by the agent if the certificates do not match.

Security Levels
The collector supports 3 different security levels as well as IP-level access lists to ensure that only authorized hosts are able to connect to the collector. The security levels are accumulative: A medium
security level requires that checks from the basic security level pass, a **high** security level requires that check from both the basic and medium security levels pass.

Network-based authorizations (authorized and blocked networks) are always evaluated before a further check based on the security level is performed.

### Basic

Lets any EventSentry agent with a valid shared secret connect.

### Medium

The remote host name (which is sent by the agent in an authorization packed based on the agent's host name) must be in an EventSentry group in order to connect.

### High

A reverse IP lookup of the connecting host must resolve to a host in a group. For example, if a host with IP address 192.168.1.50 connects, then the collector will attempt to perform a reverse lookup and will then attempt to find the resulting host name in an EventSentry group.

### Reset Certificate

Resetting the collector certificate is only necessary under the following circumstances:

- The certificate has been compromised and needs to be replaced
- The certificate needs to be replaced with a different certificate
- The remote hosts have a different certificate for the collector host cached and are rejecting the collector

When resetting the certificate, the following actions are performed:

1. The existing certificate is renamed (to preserve the certificate)
2. A new certificate will be created when the EventSentry Collector is restarted
3. Remote agents will be authorized to accept a new certificate for up to 1 week

After clicking the "Reset Certificate" button, the following actions need to be performed:

1. The configuration needs to be pushed to all remote hosts
2. The EventSentry Collector service needs to be restarted

### Reset Shared Secrets

Resetting shared secrets is only necessary if a remote EventSentry agent is re-installed without being prior being removed from the configuration. Clicking the "Reset Shared Secrets" button will erase the entire local shared secret database and accept new shared secrets from all remote hosts, as if they are connecting for the first time.

### Network Authorization

Authorized and blocked networks can be specified to either:

- allow only certain hosts or subnets access
- block certain hosts or subnets
- both

### Authorized Networks


### Blocked Networks
Specifies all subnets/hosts which will not be allowed to connect. Blocked hosts always take precedence over authorized hosts.

4.2.2 Multiple Collectors

Despite the redundancy feature available in the collector and agents, setting up more than one collector can be advantageous when regular, scheduled downtime of the host running the collector is anticipated and minimum disruption is required.

The steps below outline how to setup & configure an additional collector.

1. Determine a host
Select a host which has sufficient memory & cpu resources available to run the collector service. Windows 2012 and later is preferred since it offers better security when modern clients connect. A host with a fast connection to the back-end EventSentry database should be preferred.

2. Configure EventSentry
On the host where EventSentry is installed, open the management console and click on the "Collector" icon. In the "Hostname(s)" field append a comma and the host name of the new collector, e.g. esmain.yourcompany.com,esbackup.yourcompany.com

3. Enhanced Security
If one or more database actions which will be used by the collector are configured for enhanced security then the host designated for the backup collector will need to be configured as a trusted host.

4. Push Configuration / Deploy Agent
If the host designated for the backup collector is already running an EventSentry agent then simply push the configuration, otherwise deploy an agent with remote update. This is required.

5. Copy required files
From the EventSentry installation directory (usually C:\Program Files\EventSentry), copy the following files (and/or directories) to any temporary directory on the remote host. We will use the directory C:\EventSentry for this purpose.

   - eventsentry_gui_x64.exe
   - es_collector_svc_x64.exe
   - Qt5Core.dll
   - concrt140.dll
   - msvcp140.dll
   - vccorlib140.dll
   - vcruntime140.dll

   Example: You should have the file C:\EventSentry\x64\Qt5Core.dll.

6. Collector service registration and installation
Start the management console (eventsentry_gui[\_x64].exe) and navigate to the collector dialog. The host name field should contain the correct information entered in step (2). If not, attempt to push the configuration again and optionally restart the EventSentry agent service.

Then, click the "Install" button and point to the temporary directory.

7. Customize
It is not recommended to change the "Communication" settings of the collector, since they should match the settings of the primary collector. The "Network Authorization" settings may be customized on a backup collector if only select subnets should be allowed access.
8. Activation
The backup collector is activated by starting the service with the "Start" button. The configuration needs to also be pushed to all remote hosts from the host where EventSentry is installed (not from the backup collector), so that the remote hosts are aware of the backup collector.

9. Maintenance
The binary utilized by the collector, `es_collector_svc.exe` or `es_collector_svc_x64.exe` respectively, need to be manually update on any listed backup collector whenever a patch or a new version of EventSentry is installed. Simply stop the `EventSentryCollector` service on a backup collector, replace the binary with the latest version from the installation directory, and restart the `EventSentryCollector` service.

When multiple collectors are configured, an agent will always attempt to connect to the listed collectors sequentially, starting with the first listed host. If a connection is established with a backup collector, the agent will continue to communicate with that collector until the connection is interrupted or the agent is restarted.

4.3 Packages
EventSentry allows you to configure Filter, Health, Security & Compliance as well as Validation Scripts packages. A package contains a set of instructions (e.g. event log filters, disk space settings, service monitoring settings, etc.) that can then be applied to

- All computers
- Computers in a certain group
- Computers matching certain criteria (OS, platform, running a service)
- Individual computers only

Please see Package Options for more information on packages.

Package Types
EventSentry comes with 5 different types of packages:

1. Event Log Packages
   Contain one or more include filter, exclude filter and folder. Please see "Event Log Monitoring" for more information.

2. Log File Packages
   Contain options to monitor one or more file(s) and consolidate and/or log parsed text to the event log.

3. System Health Packages
   System Health Packages may contain the following health monitoring features:
   - Service Monitoring
   - Disk Space Monitoring
   - Folder Monitoring
   - Performance Monitoring
   - Software/Hardware Inventory
   - Process Monitoring
   - Application Scheduler
   - Event Log Backup
• File Monitoring
• Scheduled Tasks
• NTP
• System Status Tray App

Please note that a health package may only contain a maximum of one object of each type, for example you cannot add two service monitoring objects to the same health package.

4. Security & Compliance Packages

Security & Compliance packages may contain the following objects:

• Processes
• Console Logons
• Network Logons
• Account Management
• File Access
• Policy Changes
• Print Activity

Please note that a tracking package may only contain a maximum of one object of each type, for example you cannot add two process objects to the same package.

5. Validation Scripts Packages

Contain a scripts object that allows for the scheduling of one or more validation script either by tag or name.

4.3.1 Package Options

Every package, regardless of its type, includes the following configuration options.

You can view and edit package options either by right-clicking a package and selecting “Edit” or by left-clicking a package and clicking “Edit Package Options” on the right screen.

Enabled package
You can enable/disable packages to enable or disable all monitoring options contained in them. Disabled packages are shown with a red x in the tree.

Global Package
Instead of assigning a package to all groups or computers, you can make a package global. Global packages apply to all computer, regardless of their group membership. Once a package has been made global it cannot be assigned to groups or computers.

Filter Chaining Package
Indicates a package which is configured for filter chaining.

Description
Enter a description for a package to briefly describe the package, its contents and/or its purpose.

Package Assignments
You can either assign a package to a computer or groups, or configure a package to be global and thus apply to every computer in your configuration. Check the "Global Package" checkbox to make a package global, or click the "Assign" button to assign this package to one or more computers.

You can also right-click a package to configure the package assignments.
Overrides
Many features in EventSentry are bound to a particular action. Rather than configuring every event log filter, health etc. feature to use a particular action you can set the notification on a package level instead. If you set a notification on a package level then you will not be able to set the action(s) on the individual items inside the package.

To specify actions on a package level, check the “Override actions of all objects in this package” checkbox and populate the “actions” list. Please note that only event log packages may contain more than one action, health and security & compliance packages may only have one action in the list.

Use group-specific database action: When configured in the group properties, dynamically adds that database to the list of actions. The list of actions should be empty if only the group-specific action should be used for the package.

Event Log packages offer additional package options which are explained in the Event Log Packages chapter.

Packages configured for dynamic-activation still need to be assigned to groups or computers, unassigned packages will not be activated.

Dynamic Activation
You can make a package dependent on the existence of a particular Windows service or the version of Windows installed. For example, you can activate a package only if the “mysql” service is installed, or on computers running Windows Server 2008 or later. It is important to note that dynamic activation will not assign packages, as such, dynamic activation still requires the package to be assigned. Generally speaking it's recommended to make packages that utilize dynamic activation global.

All conditions need to be satisfied (in an AND like fashion) when multiple conditions are configured (e.g. Operating System and Platform).

Activate based on installed service
To activate a package only when one or more services are installed, enter the service key names in the “Installed Service(s)” field. Separate multiple service key names with a comma. When multiple services are listed then it is sufficient if only one of the listed service is installed.
Always specify the service **key name**, not the service display name.

**Activate based on an assigned tag**
Packages can be activated on hosts that have a specific tag assigned to them (either directly or implicitly through the group); separate multiple tags with a comma. When multiple tags are listed then it is sufficient if only one of the listed tags is assigned on a target host.

**Activate based on the Operating System**
To activate a package only for a specific Operating System, or range of Operating Systems, select the comparison type (at most, is, at least) as well as an Operating System. For example, when selecting "at least Windows Vista", then the package will be activated on all computers running Windows Vista or later.

**Activate based on platform**
To activate a package only for a specific platform (e.g. 64-bit), select the platform from the list or set to "any" for the package to be activated on all platforms.

**Activate based on OS type**
A package can be activated based on whether it is a domain controller, server, workstation (client) or a combination.

**Sorting Packages**
It does not matter in which order your packages are. The package order does not affect the functionality of EventSentry. You can however sort packages alphabetically (either ascending or descending) by right-clicking the corresponding package type and selecting “Sort Packages”.

### 4.3.2 Assigning Packages

Packages need to be assigned before they will be used by a computer. You can assigned to the following:

- All computers (= global assignments)
- One or more groups
- One or more computers

The EventSentry management console lets you assign packages either by right-clicking the actual packages, or by right-clicking the group or computer objects. This gives you more flexibility when configuring and working with packages.

Packages can also be assigned automatically, either depending on one or more installed service(s), or depending on the operating system of the monitored host.

**Setting packages to be global**
To configure a package as global and apply to all computers you can:

- Right-click the package and select "Global".
- Right-click the package and select "Edit" which will bring you to the package options. There, check the "Global Package" checkbox which will change the package icon accordingly.
- Right-click the "Computer Groups" container and select "Assign Package(s) ...". From this dialog you can toggle the Global flag for more than one package at one time.

[Click here](#) for more information.
Assigning packages to groups
Click here for more information.

Assigning packages to computers
Click here for more information.

Unassigned packages
Packages that are unassigned will appear gray in the package list and will not be loaded by the EventSentry agent.

4.3.2.1 Setting Packages as Global

You can configure more than one package at a time to be a global package with the "Global Package Assignment" dialog. Right-clicking the "Computer Groups" container and selecting "Assign Package(s)..." will show the following dialog:

All packages with a checked checkbox are global packages, other packages are regular packages that are already assigned or need to be assigned to a group or computer. To make a package a global...
package simply check the checkbox, to clear the global flag and make a package assignable simply clear the checkbox.

4.3.2.2 Assigning to Groups

You can assign a package to a group in two ways:

1. Right-click the package and select "Assign ..." which will bring up the "Apply Package To ..." dialog. There, select the group(s) the package should apply to and click OK. This option is preferable when you need to assign a package to more than one group.

2. Right-click the group the package should be applied to and select "Assign Package(s) ..." which will bring you to the "Package Assignments" dialog. There, select all the packages that should be applied to the selected group. This option is preferable when you need to assign more than one package to a group.
4.3.2.3 Assigning to Computers

You can assign a package to a computer in two ways:

1. Right-click the package and select "Assign ..." which will bring up the "Apply Package To ..." dialog. There, select the computer(s) the package should apply to and click OK. This option is preferable when you need to assign a package to more than one computer.

Please note that global packages will appear bold in the package list and cannot be assigned/unassigned.
Please note that global packages and packages assigned to the group the computer is a member of will appear bold. You can block package inheritance by clearing the checkbox of a package that appears in bold. Click here for more information.

2. Right-click the computer the package should be applied to and select "Assign Package(s) ..." which will bring you to the "Package Assignments" dialog. There, select all the packages that should be applied to the selected computer. This option is preferable when you need to assign more than one package to a computer.
4.3.2.3.1 Blocking Package Inheritance

Starting with version 2.90 it is possible to exclude one or more computers from global or group package assignments.

This is useful for example when you have a global package that applies to 99% of all computers, or a package assigned to a group which applies to all computers in the group with a small number of exceptions.

While it is possible to change the global or group-based assignments by assigning the package to computers directly, this runs the risk of new computers not being assigned the correct package. Instead, you can keep the global or group-based assignments and simply exclude the computers you do not wish to assign the package to.

To block inheritance for a global or group-based package assignment, expand the Computer Groups containers and navigate to the computer for which you wish to block the inheritance. Right-click the computer and select Assign Package(s)… . The resulting dialog will show you all packages that are assigned to this computer, with inherited packages being displayed in bold. To block inheritance, simply clear the check box next to the (bold) inherited package, as shown for the Services for Vista Win2k8 package below:
Blocking Inheritance

Keep in mind that blocked packages are associated with the computer item, and remain blocked even when the inherited package is toggled to be global or group-based package.

4.3.3 Downloading Packages

NETIKUS.NET offers a default set of filter and health packages that are constantly updated and improved to offer common filter and service settings.

A default set of filter and health packages is automatically configured when you first install EventSentry, and you can receive the latest up-to-date packages by downloading them from our website, directly from the management console.

1. Downloading New Packages

To download the latest packages, select Download Latest Packages ... from the Tools menu, click the icon on the toolbar or right-click the Packages container and select Download Latest Packages ...which will display the following dialog:
If you check the **Do not merge downloaded packages** ... checkbox, then new filters in updated packages will not be merged with your current packages, and you will only be able to install completely new packages.

The package file will be downloaded after you click the **Start Download** button, click the **Continue** button to select which packages should be imported.

### 2. Selecting packages to import

Once the package file has been downloaded, EventSentry will determine which packages are new and which packages have been updated since the last download.

You can select which packages you would like to import in the **Package Import Details** dialog. If you prefer not to install a particular package then you can simply clear the checkbox next to the name of the package.
Since all filters require at least one action to be associated with them, you will need to select an existing action in the Default Notification container. You can change or extend this setting after the import by right-clicking the imported package(s) and selecting Edit Options.

When importing health packages it is also recommended that you specify a default database-type notification on a package-level.

3. Post-Import Customizations
   You may edit downloaded packages (and filters) after you imported them, for example to change the description or add/change the notifications.

   It is not recommended that you rename or delete filters contained in packages however, since those filters will be imported again when you download packages the next time.

Proxy Server
   All features in EventSentry that download files or submit content through HTTP support a proxy server. If your network requires the usage of a proxy server for HTTP communication then please see Web Reports & Proxy for more information on how to configure this feature.
4.3.4 (Un)Hiding Packages

You can hide packages that you are not interested in, for example if you use EventSentry to solely monitor servers then you can hide the **Laptops** package. Hidden packages are still active and processed, but will not be shown in the management console. This feature is particularly useful when you download packages from the web.

**Hiding vs. Deleting**

If you delete a previously downloaded package from your configuration, then you will be prompted to import this package again the next time you download packages from the web. If you hide the package however then you will not be prompted to import the package in the future (unless it has been updated) since the package is technically still installed.

**Hiding a Package**

To hide a package, right-click the package container and select Hide. The package will immediately disappear from the list. The package will continue to be assigned unless you unassign it.

**Unhiding one or more Packages**

To unhide one more more packages, right-click the Packages container and select Unhide Packages which will display the following dialog:
Select the package(s) to unhide and click OK. The packages will now reappear in the tree.

4.4 Actions

With an action (up to 128 can be created) you specify how you will be notified when a relevant event occurs. The following notification types are currently supported:

- Email (SMTP)
- Database
- HTTP
- File (including plain text, (X)HTML and CSV files)
- Syslog (UDP / TCP)
- SNMP Traps
- Network Message
- Process
- Sound
- Desktop
- Service
The SMTP, HTTP, Syslog TCP and database notifications support local caching which can re-notify (e.g. SMTP server is temporarily down) a failed action when it is available again. All actions supported by the collector also support local caching.

4.4.1 Managing Actions

To enable / disable an action
Actions can be enabled and/or disabled by right-clicking the respective action icon in the navigation tree on the left. This feature is convenient if you make use of the "apply to all actions" feature in filters. Rather than modify multiple filters, you can simply de-activate or re-activate actions by clearing or checking the check-box.

Use Collector
Enabling “Use collector” routes an action through one of the configured collectors. Only select actions can be routed through the collector.

To add a new action
- right-click Actions in the left pane and select Add Action, you will be prompted for the action name
- Use the ribbon to add a new action (will prompt the “Action Selection” dialog)
- Use the ribbon but click the down-arrow of the “Add Action” button to select an action type to add

The action type (e.g. Email) cannot be changed after an action has been created.
To edit an action
- left-click (or double-click, see usability) the action item in the left pane
- right-click the action object and select Edit

The action details will then be loaded into the right pane and the active action object in the left pane will become bold. Please note that you cannot change the action type of existing action.

To delete an action
- right-click the action and select delete from the menu
- select the action and choose “Delete” from the ribbon
- select the action object and press the Del button on the keyboard

If one or more filters reference the action that was deleted, then the deleted action will be removed from the filter's action list. A filter will be disabled if the deleted action was the only action of that filter.

Finding filters referencing an action
You can view a list of all filters that are either directly or indirectly (a filter configured to trigger all actions) referencing a action. Right-click the action in question and select “Show Filters” -> “(Directly) Referencing this action”

To rename an action
• right-click the action and select rename from the menu
• select the action and press the F2 button on the keyboard (only works with usability set to double-click)
• left-click the action object for 1-2 seconds

**To copy & paste an action**
1. Click the action object in the left pane and make sure that it is selected
2. Click the copy symbol in the toolbar or choose Copy from the Edit menu
3. Click the paste symbol in the toolbar or choose Paste from the Edit menu

If a action object with the same name already exists then "Copy of" will be pre-pended to the name. Please note that action objects cannot be cut and pasted.

**To change the action order**
You can change the action order by dragging and dropping actions to a different position under the notifications container.

### 4.4.2 Schedule

An action schedule enables or disables an action based on the time of day and/or weekday. This is similar to filter schedules, but setting the schedule at the action can be preferable if you have many filters triggering the action (thus avoiding duplicate settings on multiple filters).

![Action Schedule](image)

To set a schedule, click the **Schedule** button and select during which hours the action will be active. Blue boxes indicate active hours, whereas white boxes indicate inactive hours. You can click on a weekday or hour of the day to toggle multiple boxes at once.
4.4.3 Action Options
Several generic options can be set for actions regardless of its type.

Thresholds
Action thresholds can limit how often an action is triggered. Thresholds can also be controlled with filters, which is generally preferable.

Frequency
Instead of an action being immediately triggered when a matching event occurs, the frequency of some action can be adjusted.

Action Activity
Enabling an action trigger history keeps track of when an action was triggered, including delivery information like recipients.

Dynamic Content Enhancement
Enhances emails by supplementing dynamic data in emails, currently IP addresses, with additional information like geolocation or host names.
4.4.3.1 **Thresholds**

You can limit the number of events that are passed on to an action using filter thresholds, which works well in most scenarios and offers a lot of advanced configuration settings for threshold settings (e.g. event log logging etc.).

In some cases it might be more desirable to apply a limit to an action instead. This is useful when you have a large amount of filters sending events to an action (and it would be time-consuming to setup thresholds on all of them), or if you have an action (e.g. a pager) where you need to ensure that only a limited number of events are forwarded to the action.

By setting limits on actions, you can ensure that the action will at most be triggered the set amount of times in the configured time period, regardless of how many events are being passed to the action by one or more filters. Click the **Options** button to set an action threshold.

Action thresholds can either be evaluated on the agent or on the collector (if a collector is enabled). When set to "Enabled (collector)", the threshold is global and applies to all emails sent by the collector. As such, a limit of "10 per 1 hour" would result in no more than 10 emails being sent in an hour. If the same threshold is configured for "Enabled (agent)", the threshold is evaluated on the agent and means
that no more than 10 emails will be sent by each agent - which could result in more than 10 emails being sent by multiple agents.

It is important to understand that an action limit does not apply to the number of events, but instead to the number of times the action is triggered. For example, if you set a limit to an Email action, then the limit will apply to the number of emails, not the number of events inside the emails. As such, the action limit feature works differently depending on the type of action that is being triggered. Please see the list below for more details on how the action limit works for different action types:

<table>
<thead>
<tr>
<th>Action Type</th>
<th>Per Event</th>
<th>Per Trigger (Detail)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (SMTP)</td>
<td>-</td>
<td>Yes (per email)</td>
</tr>
<tr>
<td>Pager (SNPP)</td>
<td>-</td>
<td>Yes (per connection to SNPP server)</td>
</tr>
<tr>
<td>Database</td>
<td>-</td>
<td>Yes (per connection to database server)</td>
</tr>
<tr>
<td>Syslog</td>
<td>-</td>
<td>Yes (per connections to Syslog server)</td>
</tr>
<tr>
<td>File</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Parallel</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Network</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Message</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Process</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Sound</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Desktop</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Jabber</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>SNMP</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Service</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Yes</td>
<td>-</td>
</tr>
</tbody>
</table>

**Action Thresholds with collector**

Note the following when using collector-side action thresholds:

- Collector-side action thresholds are currently only supported for the SMTP action.
- If an email is the last email before the threshold is exceeded, the email subject will begin with `[THRESHOLD REACHED]` to indicate that some emails may be suppressed.

**Frequency**

By default, the email, pager and database actions forward events to the configured server every 5 seconds. This interval can be increased for the purpose of aggregating events. For example, instead of getting 3 emails within a minute each including a single event, you can get 1 email every minute which contains all three events. This feature is mostly useful for the email and database action.
4.4.3.2 Frequency

The action frequency (or polling interval) specifies how often events which have been submitted to an action will be processed (and sent to its respective destination) by that action. For example, if the action frequency for an email is set to 60 seconds, then the EventSentry agent will never send more than one email per minute because the events will essentially be grouped together. 3 events happening 5 seconds apart will all be sent in one email.

The action frequency applies to the following action types:

- Email
- Database
- Syslog
- HTTP
- Network
- SNPP

4.4.3.3 Action Activity

You can track whenever a certain action is being triggered by clicking the Options button on an action dialog. The trigger history feature is currently available for all low-volume actions, including Email, Jabber and SNPP.

When enabled, EventSentry will record every time the action is triggered, including the timestamp as well as recipient information of the action. The action trigger history can be reviewed using the web reports on the "Event Search -> Action History" page.

The fields listed below are recorded in the history:

- Source Computer
- Action Name
- Action Type
- Action Recipients
- Filter Package Name
- Filter Name
- Event Number
- Event ID
- Event Log
- Event Source
- Event ID
4.4.3.4 Dynamic Content Enhancement

EventSentry can automatically extract IP addresses from any event and supplement the IP addresses with reverse lookup and/or Geo IP lookup data. Providing geolocation and/or host names inside the email makes the usability of email alerts for the recipient significantly more useful without requiring the recipient to perform manual lookups.

The picture below shows an email alert which contains an IP address (blue rectangle) that has been enhanced by providing additional context. Immediately following the IP address is a reverse lookup (green line) as well as the geolocation of the IP address (blue line).

This feature is currently only available for email actions which utilize the collector. Both reverse lookup and geoip lookups are performed on the collector, not the agent.

4.4.4 Email (SMTP)

A SMTP action forwards event log messages via email. The email actions supports multiple formats, backup SMTP servers, SSL authentication, variables and more.
**Sender Name**
This value will appear as the sender name of the email (not the email address). This is usually the hostname of the computer. If you plan on replicating a SMTP action to multiple hosts then you can use the $HOSTNAME variable here. To learn more about variables click [here](#).

**Sender Email**
The email address under which this email will be sent. If you are notifying people other than yourself then you should probably make sure that replies to emails sent from EventSentry arrive somewhere.

**Recipients**
A comma-separated list of the recipient's email addresses. The total length of all recipients (including the commas) can not exceed 512 characters. If any of the email addresses are rejected by the server then the email will not be sent and an error will be logged to the event log.

You can click the mobile phone icon next to the recipients field if you intend to send a text message to a mobile phone through an email gateway. Most mobile phone providers offer such gateways free of charge to the sender, even though standard text messaging rates usually apply to the recipient. The helper dialog creates the correct email address for you, if your provider is not listed then you will need to contact your provider to obtain the correct email address.
Please feel free to suggest additional mobile phone providers to our support team for inclusion in a future version of EventSentry.

As stated in the dialog, it is highly recommend that you apply threshold to any action that sends messages to a mobile / cell phone where per-message charges might apply.

**Subject**

The subject of the email. The variables $LOG$ and $COUNT$ are supported. To learn more about variables click here.

**Dynamic text in subject**

If at least one event of the current email has been spooled by the agent because the SMTP server was temporarily unavailable, then the text [BACKUP] will be automatically added to the subject. If at least one event of the currently email is from an event log rescan (e.g. the event occurred while the agent was not running), then the text [RESCAN] will be automatically added to the subject.

If the action has a collector-side threshold configured and an email is the last email before the threshold is exceeded, then the subject will be modified to start with the text [THRESHOLD REACHED] to indicate that some emails may be suppressed.

**(Primary) SMTP Server and Port**

The host name or IP address of the SMTP server and the port on which the specified SMTP server listens for incoming requests. The port is set to 25 by default.

**(Secondary) SMTP Server and Port**

You can specify a secondary SMTP server (including port and authentication information) that will be contacted if the primary SMTP server is unavailable. EventSentry will always connect to the primary SMTP server before it will try the secondary SMTP server.

**SMTP Authentication Username / Password**
If your SMTP server requires authentication then specify username and password here. You can specify a username and password for both the primary and the secondary server.

Currently the clear text (AUTH LOGIN) and MD5 (CRAM MD-5) authentication protocols are supported.

**TLS**
Set this option to either **TLS** or **TLS (verify)** if the server that you are connecting to supports or requires a TLS connection. Setting this option to **TLS (verify)** will only connect to remote SMTP servers that have a valid TLS certificate, setting this option to **TLS** will accept any remote certificate, including self-signed ones.

**Style**
You can receive emails either as plain text, in HTML format or in miniature size.

*Plain Text:* Sends emails without any formatting.

*HTML Email (Legacy & Modern):* HTML emails can be sent in the legacy and the modern format. Legacy format is the original HTML format, the modern HTML format was introduced with version 3.0. When using the HTML (Legacy) option you can also configure the font and size used in the HTML emails, the default is **Verdana** at **11px**.

Emails sent in HTML format also include a plain text for non-html capable email clients.

**Display & Delivery Options**
It is possible to customize the content and look of email actions, including which event log properties are included in emails sent by EventSentry.

**Header / Footer**
You can optionally add a header and/or footer to every outgoing email using this notification. This feature is especially useful for service providers who wish to add additional information to emails sent to their customers. Both the header and footer may contain up to 1024 characters, with a maximum of 2048 after variable expansion.
High and Low Importance
Most email clients support importance flags that indicate the importance of an email. This feature is useful to immediately determine if an email sent by EventSentry is important or not.

- **High Importance:** Emails will be sent with the high importance flag if at least one event log entry in the email is either an error or an audit failure.
- **Low Importance:** Emails will be sent with the low importance flag if an email contains only information or audit success messages.

Flag Literal
Used in combination with the High and Low Importance flags. When Flag Literal is checked, an email will always be sent with either a high or low importance, regardless of the email content.

Max. number of events per email
By default EventSentry would include as many event records as scanned in an email (an email could contain 5+ event records if those occurred in a short amount of time). This option is particularly useful for cell phones where event records after the first one cannot be read. Set this option to unlimited to restore the default behaviour, otherwise to the maximum number of event records each email should contain.

Dial-Up Connection
You can select an existing RAS (including VPN) connection, and EventSentry will dial this connection prior to sending the email, if the SMTP server could not be contacted. The RAS connection will be hung up after sending the emails if the "Hangup After" option is checked.

![Dial-Up / VPN Connection](image)

You can paste the basic event properties from an email directly into the General Filter dialog to easily create an include/exclude filter based on an email you received.

Simple select the event in the email and copy it to the clipboard. Then, create a filter (or open an existing filter), click on any text field and press CTRL+V. The keyboard combination is necessary, a right-click & paste will not work. Click here for more information.

### 4.4.4.1 Troubleshooting Email (SMTP)

Solutions for common problems with the SMTP action:

- Make sure the primary (and the secondary if applicable) hostname are entered correctly, including the port (25 by default). Also make sure that the host where EventSentry is installed can reach the specified hostname.

- You can separate multiple recipients with a comma ( , ), make sure there are no spaces in this field.

- Make sure the specified SMTP server will accept messages from the specified Sender Email address and the computer where EventSentry is installed.

- This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>Unable to connect to specified SMTP server.</td>
</tr>
<tr>
<td>501</td>
<td>An error occurred during SMTP communication.</td>
</tr>
<tr>
<td>502</td>
<td>Unable to connect to primary SMTP server, backup host will be tried.</td>
</tr>
</tbody>
</table>

### 4.4.4.2 Display & Delivery Options

**Style / Customize**

The look and feel of emails can be customized by choosing the font and size used in HTML emails, by selecting which event properties should be included in the email, or by minimizing the amount of text that is displayed in the email altogether.

**Plain Text Style**

Emails will be sent in plain ASCII text. Clicking the Customize button will allow you to pick which fields from an event are included in the email. For example, you can customize the output to never show the event number or never show the event category for example.

**HTML (Legacy) Style**

Use the HTML Font Options to customize the font and font size of emails generated by EventSentry. As with the plain text style, clicking the Customize button will allow you to pick which fields from an event are included in the email.

**HTML (Modern) Style**
Font and font size customization are not supported in this style, event fields can be toggled. Since this style shows two fields per row (e.g. source & category), a field is only hidden if both fields in the row are unchecked. As such, just clearing the “Event Category” check box will have no effect since the event source is being displayed.

Customizing the fields which are displayed / included in an email may break the copy/paste functionality in the filter dialog.

**Miniature Style**
If you plan on being notified on a cellphone or pager then you should check this box. It sends small emails that contain only the most important information. You can customize the look of “Miniature” email by clicking the “Customize” button. The option Max. number of events per email might be of interested as well.

You can customize which event log properties (e.g. log, source, category, etc.) will be included in emails sent by EventSentry. By default, all properties with the exception of the “Filter Notes” will be included.
Checking the “Include EventSentry Version” check box will show the current version of the EventSentry agent in the email. This is an easy and unobtrusive way to verify that the agent on a given machine is running the latest version.

**Keep Space Characters**
When checked, preserves space characters from events in HTML emails.

**Footer**
Emails can include the following types of automatic footers:

- No Footer
- Agent version only: Shows the version of the agent running on the host which generated the event(s).
- Complete status summary: Includes the agent version as well as the following:
  1. Operating System
  2. IP Address
  3. Uptime
  4. CPU & Memory Utilization
  5. Logged on user(s) if any

Windows Server 2008 R2 SP1 | 21.3.103
Up 3 days and 34 minutes
CPU: 3% | MEMFREE: 31%
Logged on: TESTGROUND\[user] [RDP-Tcp#0]
EventSentry v3.3.0.109 rev105

Complete Status Summary Example
4.4.5 Database

EventSentry can send event log records to any supported database server using ODBC. Connection strings are the recommended way to point the action to a database.

See Steps to Event Log Consolidation for information on how to consolidate event log records.

Use the Database Import Utility to import archived event log backup (.evt/.evtx) or log files into a database.

Connection Strings

Applications can either use a connection string or a system DSN (data source name) to connect to a database. The former is easier to deploy since you don't have to create (and maintain) a DSN on every host.

To create the connection string, either refer to your:

- Database vendors documentation
- An online resource (e.g. http://www.connectionstrings.com)
- Use the built-in Connection String Helper by clicking on Create

The Connection String Helper will setup a connection string for supported databases automatically, you will only need to specify the required parameters. If your connection string needs additional information or does not work then please edit the generated string in the main ODBC dialog manually.

Enhanced Security
Checking this box will prevent the connection string details from being transmitted to the remote agents for additional security. This check-box should only be checked when a collector is configured, otherwise the remote agents will not be able to connect to the database.

If one or more remote hosts are running an EventSentry service other than the monitoring agent (e.g. Heartbeat Agent, Network Service), then the hosts running those services will need to be configured as a Trusted Host. Trusted hosts will receive the full connection string details, even when enhanced security is enabled. To configure a host as trusted, right-click the host item in the computer group, click “Edit” and check the “Trusted Host” check box.

After setting up a connection to your database server, click the Initialize or Update Database button to create the database and schema.

**DSN Name**
As an alternative to connection strings you can also use System DSN names to connect to a database. Enter the name of a System DSN, please see Best Practices for more information on DSN names. The DSN name specified here needs to exist on every host using this action (see also: Troubleshooting).

You cannot specify both a DSN and a connection string.

**Username / Password**
If your data source requires a login then specify username and password. For more information on username and passwords please also read Best Practices.

**Manage ODBC**
Clicking this button will bring up the Data Source Administrator, a built-in application that ships with Windows and allows you to configure System and User DSNs. Note that this button is only active when you are connected to the local machine.

**Initialize or Update Database**
Launches the Configuration Assistant, which either creates a new database or updates an existing database to the latest schema (according to schema.xml). Launching the configuration assistant is only
necessary when creating a new EventSentry action, or when the configuration assistant failed to update one more more database during an upgrade.

**General Options**

**Ignore Binary Data**
Some events, usually from either the Application or System event log, have binary data associated with them. If you are not interested in consolidating binary data in the database, then you can check this check box.

**Extended Error Logging**
By default the EventSentry agent only logs connection-related database issues to the event log. By enabling extended error logging, most database errors are logged to the event log periodically.

**Trim Windows Security Events**
Many Windows security events contain non-essential descriptions after the event details. These descriptions are the same for all events of the same event id, and can use up considerable space in a database. Activating this option will automatically remove these descriptions from the event before they are logged to the database. The event descriptions remain in place for all other notification types, e.g. email. The screenshot below shows what type of information is removed from the event based on the Windows Security event 4688 which is logged when a new process is launched:

```
A new process has been created.
Subject:
  Security ID: NETIKUS\imgmacstecher
  Account Name: imgmacstecher
  Account Domain: NETIKUS
  Logon ID: 0xCBEF7E7

Process Information:
  New Process ID: 0x1bc
  New Process Name: C:\Windows\System32\wmc.exe
  Token Elevation Type: TokenElevationTypelimited (3)
  Creator Process ID: 0x1d54
  Process Command Line:

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy:

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account, or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
```

**Always Append Binary Data - REGISTRY & ADVANCED USERS ONLY**
In some cases, especially when handling large amounts of large, unique and non-repetitive binary data, the EventSentry agents can pose a significant stress on the database server when the size of the ESEventlogData table gets too big. All binary data is stored in this lookup table, and the agent attempts to reuse existing rows in this table if it is encountering duplicate binary data, as is generally the case.

If you expect large amounts of unique binary data, then you can avoid this problem by preventing the EventSentry agent from re-using binary entries and instead appending binary data to the ESEventlogData table. This will impose less work on the database server, since the ESEventlogData table does not have to be queried as often anymore (it still has to be queried once for every binary entry).

To activate this option:

- Clear the "Ignore Binary Data" check box if it is checked
- Close the management console
- Start regedit.exe and navigate to the registry for the action you would like to activate this for:
HKEY_LOCAL_MACHINE\Software\netikus.net\EventSentry\Targets\MYDATABASE

where MYDATABASE is the name of your database action. There, add a new DWORD value with the name of ODBC_AlwaysAppendBinaryData and set the value to 1.

4.4.5.1 Setting up the database

EventSentry uses a set of tables where event log, system health, log file and "security & compliance" information are stored.

The database is setup automatically after installation through the Configuration Assistant. You can also run the Configuration Assistant at any point in time to upgrade an existing database to the latest schema. The can also launch the Configuration Assistant from the action dialog, by clicking on the "Initialize or Update Database" button.

Security Info: Both username and password are currently written in plain text to the registry. By default the EventSentry registry key is only accessible to Administrators.

4.4.5.2 Database Schema

The EventSentry database uses dozens of tables to store all collected information, and almost all tables are linked to each other.

If you intend to use third-party (reporting) applications to read information from our database, then understanding these relationships is important. Please see the following pages for a graphical display of all tables and their relationships.
4.4.5.2.1 Event Log Consolidation
4.4.5.2.2 Log File Monitoring

4.4.5.2.2.1 Non-Delimited Log Files
4.4.5.2.2.2 Delimited Log Files
4.4.5.2.3 Service Monitoring

4.4.5.2.3.1 Service Status
4.4.5.2.3.2 Service History
4.4.5.2.4 Heartbeat Monitoring

4.4.5.2.4.1 Heartbeat Status
4.4.5.2.4.2 Heartbeat History

4.4.5.2.4.3 Heartbeat Response Times
4.4.5.2.5 Nessus

4.4.5.2.6 Syslog
4.4.5.2.7 Snmp
4.4.5.2.8 Environment Monitoring
4.4.5.2.9 Compliance Tracking

4.4.5.2.9.1 Process Tracking
4.4.5.2.9.2 Logon Tracking
4.4.5.2.9.4 File Access Tracking
4.4.5.2.9.5 Account Management
### EventSentry Help v5.0144

#### EventLog/Accounting (dbo)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Nullable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventSource</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetName</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourcePort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EventLog/Accounting_Computer (dbo)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Nullable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventSource</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetName</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourcePort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EventLog/Accounting_Computer (dbo)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Nullable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventSource</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetName</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourcePort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EventLog/Accounting_Computer (dbo)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Nullable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventSource</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetName</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourcePort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EventLog/Accounting_Computer (dbo)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Nullable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventSource</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetName</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourcePort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EventLog/Accounting_Computer (dbo)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Nullable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventSource</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetName</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourcePort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EventLog/Accounting_Computer (dbo)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Nullable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventSource</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EventID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetName</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceID</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceType</td>
<td>int</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourceIP</td>
<td>varchar(255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SourcePort</td>
<td>int</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© <2002 - 2022> ... NETIKUS.NET ltd
4.4.5.2.9.6 Policy Change Tracking
4.4.5.2.10 Inventory

4.4.5.2.10.1 Software Monitoring
4.4.5.2.10.2 Uptime Monitoring
4.4.5.2.10.3 Hardware Inventory

[Diagram of database tables]
4.4.5.2.11  File Monitoring
4.4.5.2.12 Performance Monitoring
4.4.5.2.13 Disk Space Monitoring

4.4.5.3 Steps to Event Log Consolidation

Please follow the steps outlined below to consolidate event log records to a central database. Depending on the database you are using you might need to perform additional steps.

Install a Database Server
If you are not using the built-in database, and do not already have a database like PostgreSQL or MSSQL running, then you will need to setup a database server on your network. The EventSentry web site contains guides that assist with the setup process (see http://www.eventsentry.com/support/documentation) as well as a setup assistant for MS SQL Server Express that can be downloaded from http://www.eventsentry.com/downloads.

Setup a database during installation
An EventSentry database will automatically setup with the Configuration Assistant after the installation process is complete. The quickest way to setup an EventSentry database is by selecting the Built-In database during installation.

Configure Consolidation & Deploy Agents
1. Create / configure the ODBC action in EventSentry and configure it to either use a connection string (recommended) or a System DSN. Test the ODBC action.

2. Click the "Initialize / Update Database" button to setup the database for use with EventSentry.

3. Optional: If you are using a system DSN then make sure the specified ODBC System DSN exists on all machines that will write to the database. We recommend using EventSentry Admin Assistant if you need to roll out a system DSN name to multiple computers.

4. Create one or more include filters that will collect event log information and forward them to the ODBC action (database). Event log consolidation will not start until the event log filters are properly setup.

5. Use remote update to send the updated filters & actions to all hosts running the EventSentry agent (not necessary when using the collector).

6. Setup the web reports to query the database through a web browser.

4.4.5.4 Troubleshooting Databases

Solutions for common problems with the database action:

- If you are using DSN names (not recommended) then make sure that the DSN name you specified is a System DSN. User DSN names are not supported.

- The DSN name you specified must match an existing System DSN that points to the correct database. These data source names (DSN) need to be setup on every computer where the EventSentry agent/service is installed. You can use the EventSentry Admin Assistant to easily roll out data source names to multiple computers.

- Use connection strings instead of System DSNs to avoid having to setup the DSN on target computers.

- Make sure that all the necessary ODBC drivers for your database server are installed correctly on the host where EventSentry is installed. Microsoft Windows 2000 and higher ship with SQL Server drivers installed by default. All other drivers will have to be installed manually.

- The database needs to be setup and initialized as described in the previous chapter.

- This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>530</td>
<td>A specific feature is unable to connect to the database.</td>
</tr>
<tr>
<td>531</td>
<td>An error occurred connecting to the specified database.</td>
</tr>
<tr>
<td>532</td>
<td>The following errors or warnings occurred within the last 5 minutes while communicating with the database: &lt;list of errors&gt;</td>
</tr>
</tbody>
</table>

4.4.5.5 Web Reports

The web reports are the reporting tool for all data collected by EventSentry and require that one or more EventSentry databases are setup.
The web reports can either be installed as part of the main EventSentry setup (recommended), or downloaded from the customer area and installed separately. When installed separately, they can either be installed on the same machine where the main setup was run, or on a different machine. The default installation directory for the web reports is `C:\Program Files\EventSentry\WebReports`.

1a. Installation with the main EventSentry Installer
To install the web reports with the installer, make sure that the “Web Reports” component is selected. See Local Installation for more details on the installation process.

You can now navigate with your web browser to the index page, e.g. `http://yourserver:8080/

2b. Installation with the separate web reports installer
To perform a manual installation of the web reports, using the separate web reports installer (e.g. `eventsentry_webreports_v4_2_1_0_windows_setup.exe`), download the installer from the customer area and simply run the installer.

The stand-alone installer can be run on Windows, Linux and/or OS X. The web reports can be installed on any host which has direct access to the database.

An installation alongside an existing EventSentry installation is also possible, but running the main installer which includes the web reports is recommended in that case. If the web reports installer was installed along side an existing EventSentry installation, then it can be uninstalled at any time.

3. Configuration Files
All settings in the web reports are stored in XML configuration files.

- `configuration.xml`
  This is the main configuration file for the web reports and automatically configured during the product installation. The file contains all profiles properties as well as global settings for troubleshooting.

- `preferences.xml`
  This file contains all global as well as user-specific preferences.

- `reports.xml`
  This file contains a list of all available reports.

- `jobs.xml`
  This file contains a list of all configured jobs.

- `users.xml`
  Controls access control and, when enabled, a list of all users and groups.
4.4.6 Process

EventSentry can launch any external process and pass command line arguments to the process. Processes can either be visible on the desktop or run in the background.

When this notification is triggered, EventSentry will log an event to the event log indicating whether the process was launched successfully or not.

Filename
Specify the file to be executed in the Filename field. You can either specify or select an existing script with the "Browse" button, or select an embedded script with the drop-down menu. Embedded scripts are specified with the @ symbol in front of the file.

Command Line Arguments
These are custom arguments that you can pass to the process. You can use variables in this field, for example insertion strings ($STR1, $STR2, ...).

Runtime Argument 1 .. 10
Here you can pass the event record details to the process. All arguments are enclosed in quotes, only the first 768 characters of the actual event message are passed to the process.

The command line for the screenshot above could look like this:

cscript.exe c:\temp\dosprint\eventprint.vbs "Application" "Warning" "EventSentry" "Service Monitoring" 10100 ""DBSERVER" "7/27/2008 3:15:23 PM" "The status of service MySQL (MySQL) changed from Running to Stopped.

See Options for more configuration options.
4.4.6.1 Options

Process Priority
The priority of the process; normal by default.

Start this process on the desktop (visible)
If you check this box then the process will be visible when you are logged on to the computer. If this box is not checked then the process will be invisible.

Timeout
Terminates the process after the selected amount of minutes. Set this option to 00 if the process should never be terminated.

Terminate Child Processes: Terminates all child processes that have been launched by the process recursively.

Event Log Options
Similar to the Application Scheduler, the agent can log an event to the event log based on the return code (ERRORLEVEL) the process provides. This is mostly useful for console processes and scripts.

Log return code 0:
Logs an informational event when the process exited with return code of 0.

Log return code > 0:
Logs an error event when the process exited with a return code larger than 0 (usually implying an error).

4.4.6.2 Troubleshooting Processes

Solutions for common problems with the Process action:

- The LocalSystem account (or the account the EventSentry service is running under) will need permission to execute the file specified in Filename.

- The specified executable will need to be present on every computer using this notification action.

- Processes launched will not be visible on the desktop unless the "Start this process on the desktop" is checked.

- This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>561</td>
<td>The process could not be launched.</td>
</tr>
<tr>
<td>562</td>
<td>The process exceeded the maximum run time and could not be terminated.</td>
</tr>
<tr>
<td>563</td>
<td>The process exceeded the maximum run time and was successfully terminated.</td>
</tr>
</tbody>
</table>

4.4.6.3 Event Log

The following events are logged by this feature when a process is launched successfully:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>560</td>
<td>The process was launched successfully (logged after process has exited gracefully).</td>
</tr>
<tr>
<td>564</td>
<td>The process was launched successfully.</td>
</tr>
</tbody>
</table>

4.4.7 Syslog

You can send event log records to remote Unix/Linux Syslog servers either through the UDP or TCP protocol. Event log records can be sent in a variety of formats, including Snare, Graylog, CEF and others.

<table>
<thead>
<tr>
<th>Required</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname: syslogcollector</td>
<td></td>
</tr>
<tr>
<td>Port: 514</td>
<td>Protocol: TCP</td>
</tr>
<tr>
<td>Format: RFC 5424</td>
<td></td>
</tr>
</tbody>
</table>

Hostname
- The IP address or host name of the remote Syslog server.

Port
- The port on which the remote Syslog server is listening for incoming requests, 514 by default.

Protocol
- The protocol to use, either UDP or TCP. Most hosts use the UDP protocol.

Use TLS
- Use TLS encryption when supported by the remote Syslog server, requires TCP.
Format
The format in which event log records are sent. The “EventSentry” format is shown below:

Direct (without collector):
hostname: optional prefix[timestamp-eventnumber]

Indirect (through collector):
hostname: optional prefix[timestamp-eventnumber]

Event category, event user and binary data are only included if they are present in the event record. Carriage returns in the event log record are removed automatically.

Other supported formats are Snare, RFC 5424, Graylog (GELF), CEF, Nagios Log Server as well as a custom JSON format.

Criticality (Snare format only)
When the “Snare” format is selected, configure a criticality

Prefix
You can have a text string prefix every Syslog message that is sent out by EventSentry. Simply enter the string into the Prefix field.

Delimiter
By default, all fields from the event log are concatenated with a colon (:), but a different delimiter can be specified.

Convert log text to UTF8
Converts the event log message to UTF8 format.

Include event binary data
Includes event binary data, if any, in the Syslog message.

Include Structured Data (RFC 5424 only)
Includes key event fields as structured data in addition to the Syslog message.

Compress
Compresses data, only support for the GELF format via UDP
Most Syslog daemons on Unix/Linux servers do not accept remote Syslog packets by default. Please read the according man pages if you do not know how to enable this feature. On most Linux distributions you will need to either pass the `-r` or `-x` option to the Syslog daemon upon startup.

### 4.4.7.1 Troubleshooting Syslog

Solutions for common problems with the Syslog action:

- Make sure that the syslog server you are sending to is configured to accept remote connections
- Make sure that the syslog server you are sending to is configured to use the same protocol and port as specified in **Protocol** and **Port**. This is usually the **UDP** protocol with port **514** but can be different.
- This action logs the following events to the application event log with the **EventSentry** event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>520</td>
<td>A TCP connection could not be established with the remote host.</td>
</tr>
<tr>
<td>521</td>
<td>A UDP socket could not be created.</td>
</tr>
</tbody>
</table>

### 4.4.8 SNMP

You can send v1, v2c or v3 SNMP traps to a SNMP management station.

**MIB**

In order for traps to be displayed correctly in your SNMP management system, you will need to import/compile one of the two MIBs that are shipped with EventSentry:

- EventSentryV1.mib
- EventSentryV2cV3.mib

These files are installed in the "Mibs" sub directory of the installation directory of EventSentry (`C: \Program Files\EventSentry\Mibs` by default). Depending on the version of trap you are sending, you will need to import either one:

- Version 1: EventSentryV1.mib
- Version 2c & 3: EventSentryV2cV3.mib

**Common Settings**

![Common Settings](image)

**SNMP Version**

The version with which the SNMP trap will be sent.

**Hostname**

The host name or IP address of the machine running the SNMP management application.

**Port**

The UDP port to be used, 162 by default.

**Test**

Sends a test trap to the configured management station.
SNMP v1/v2c Settings

Community
   The SNMP community string.

SNMP v3 Settings

If the receiving management station supports v3 SNMP traps, then you configure some of the advanced SNMP options, such as authentication and encryption, that are only available in SNMP v3 traps.

![SNMP v3 Settings GUI](image)

**Authentication (Data Integrity)**

Select one of the available authentication mechanisms (MD5 (96bit) or SHA (96bit)) or select "None" if no authentication/data integrity is desired. A password must be entered when authentication is selected.

**Encryption (Privacy)**

Select one of the available encryption algorithms (DES, 3DES or AES (128 bit)) or select "None" if no encryption is desired. A password must be entered when encryption is selected.

**EngineID**

SNMPv3 requires an engineID, which is a unique identifier for a SNMP engine (such as EventSentry). EventSentry can either generate the engine ID automatically, using either the MAC or IP address of a network interface, or you can manually specify the engine ID. On multi-homed hosts, the MAC or IP address of the interface sending the trap is used when the engine ID is automatically generated.

### 4.4.8.1 Troubleshooting SNMP

Solutions for common problems with the SNMP action:

- Make sure you import the EventSentry MIB on the target host. The EventSentryV1.mib file is located in the Mibs sub directory of the installation directory.

- Make sure the SNMP management console supports SNMP v1 traps.

- This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>590</td>
<td>A trap could not be sent.</td>
</tr>
</tbody>
</table>
4.4.9 Pager (SNPP)

You can forward event log message to your pager if your provider supports the SNPP protocol. The SNPP protocol is a simplified version of the SMTP protocol and allows you to send messages to pager using TCP/IP over the Internet.

To find out if your provider supports SNPP you might want to check your provider's web site or visit http://www.notepage.net/snpp.htm which contains a list of most paging providers in the US including their SNPP server details.

Required Settings

<table>
<thead>
<tr>
<th>Hostname: snpp.skytel.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port: 7777</td>
</tr>
<tr>
<td>Pager ID: 123456</td>
</tr>
</tbody>
</table>

Hostname

The host name of your provider's SNPP server, check with your provider to find out whether they offer SNPP to their customers and what their SNPP server is or visit http://www.notepage.net/snpp.htm.

Port

The TCP port the SNPP server is listening on, usually 7777 or 444.

Pager ID

The number of the pager.

Customize Fields

You can configure which event details will be sent to the pager by clicking the Customize Fields button. This feature is identical to the Customize Mini feature found in the email notification action:

Select which fields in which order you would like to have sent to the pager and click OK.
4.4.9.1 Troubleshooting SNPP

This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>600</td>
<td>A connection with the remote SNPP host could not be established.</td>
</tr>
<tr>
<td>601</td>
<td>A message to the specified pager recipient could not be sent.</td>
</tr>
<tr>
<td>602</td>
<td>Unable to send message.</td>
</tr>
</tbody>
</table>

4.4.10 Service & Process Control

EventSentry can control a service or kill a process in response to an event log entry.

Service Control Mode

**Service Name**
Name of the service which should be controlled.

**Action to perform**
The type of action to perform on the service (start, stop, restart, continue, pause are supported).

Process Kill Mode

**Process Name**
Name of the process that should be terminated. You can use insertion strings such as $STR1, $STR2 etc. here. This field accepts PIDs in both decimal and hex representation as well as process names so that it can easily be linked directly to events like event id 4688. Please note that the pull-down menu only lists processes on the local machine.

**Kill Multiple Instances**
By default, only the first process found that matches the specified name will be terminated. Checking this box will terminate all processes that match the name specified in Process Name.

**Kill Child Processes**
Terminates all child processes, recursively, of Process Name that have been launched by the process.
4.4.10.1 Troubleshooting Service Control

This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>611</td>
<td>Unable to connect to the SCM (Service Control Manager).</td>
</tr>
<tr>
<td>612</td>
<td>Unable to open requested service.</td>
</tr>
<tr>
<td>613</td>
<td>Unable to send request service control command.</td>
</tr>
<tr>
<td>614</td>
<td>The service could not be restarted because it could not stopped.</td>
</tr>
<tr>
<td>615</td>
<td>Service control command was sent successfully, but service not in desired state.</td>
</tr>
<tr>
<td>617</td>
<td>The specified process could not be terminated.</td>
</tr>
</tbody>
</table>

4.4.11 File

EventSentry can write (append) event log records to ASCII, XHTML or CSV files. Just specify the filename and the type of output (ASCII, XHTML or CSV) you would like.

**Filename**
The name of the output file. The file will be created if it does not yet exist; the directory will not be created automatically and has to already exist. This fields does support runtime variables, to learn more about variables click here.

If you choose XHTML as the file type and have an existing action file (not created by EventSentry), then the specified file will be overwritten.

**Delimiter**
Specify a delimiter, the default delimiter is a comma.

**File Type**
The desired output format: Plain, (X)HTML or CSV.

When using the (X)HTML option you can also configure the font and size used in the (X)HTML emails. The default is Verdana at 11px.

Click here to view a Frequently Asked Questions entry for this action.
4.4.11.1 Troubleshooting Files

Solutions for common problems with the File action:

- By default EventSentry will not be able to write to a file that is located on a remote server (shared drive) due to permission issues. The EventSentry service runs under the LocalSystem user account, an account that usually does not have any permissions on remote computers. Please refer to the troubleshooting FAQ for a solution to this problem.

- The directory for File Name will have to exist and will not be created by EventSentry. The file name itself will however be created if necessary.

- This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>510</td>
<td>The requested file could not be opened/created.</td>
</tr>
</tbody>
</table>

Also, it is generally not recommend to use one file name for multiple installations of EventSentry due to possible timing problems. If more than one instance of EventSentry tries to write to the file at the same time, then some event records could be skipped or the file could become corrupted.

4.4.12 Shutdown / Reboot

EventSentry can restart or shutdown a computer.

**Force**
An application with unsaved changes might prevent the computer from being rebooted or shutdown. Check this box to force applications to close.

**Timeout**
Specify the number of seconds EventSentry should wait before the computer is restarted or rebooted.

4.4.12.1 Troubleshooting Shutdown/Reboots

This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>620</td>
<td>A system shutdown/reboot could not be initiated.</td>
</tr>
</tbody>
</table>
4.4.13 Jabber

You can forward event log messages as Instant Messages through the Jabber protocol. EventSentry supports plain text as well as messages encrypted through TLS/SSL. Just specify a server, login and recipient and EventSentry will instantly notify you of critical event log messages.

![Jabber configuration settings](image)

**Server**
- The host name or the IP address of the Jabber server.

**Port**
- Specify the TCP port of the Jabber server.

**Use TLS/SSL**
- Check this box if the server requires or supports TLS/SSL.

**Username**
- The Jabber ID required to log into the jabber server. Check with your server administrator to determine the correct login.

**Password**
- The password for "Username".

**Recipient**
- The recipient that will receive the instant message on the Jabber server. This can also be a chat room (see below).

**Use Multi-User Chat (chat room)**
- Check this box to send jabber messages to a chat room instead of directly to another user.

**Alias**
- Most chat rooms require an alias, specify it here.

### 4.4.13.1 Troubleshooting Jabber

Solutions for common problems with the Jabber action:
- Make sure that you are using the correct login. Logins for Jabber vary and can be a username or email address.

- If your server requires TLS/SSL (e.g. talk.google.com), then make sure that you check the "Use TLS/SSL" check box

- This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>630</td>
<td>A connection to the Jabber/XMPP host could not be established.</td>
</tr>
<tr>
<td>631</td>
<td>A message could not be sent to the chat room.</td>
</tr>
</tbody>
</table>

### 4.4.14 **Http**

The HTTP action can interact with public HTTP-based APIs like ticketing systems, collaboration suites and hardware devices in a number of ways:

- Submit a form
- POST data
- PUT data
- GET request

The HTTP action supports both HTTP and HTTPS, authentication (Basic, Digest and NTLM) and allows for up to 20 form elements to be submitted. Form elements can either contain static information, or dynamic information through the use of variables.

Note that the HTTP action can not only be triggered by events (like all other actions), but also by the System Tray Utility to facilitate the creation of support tickets in web-based ticketing system.

The HTTP action can either be configured to submit data to a HTTP-based form (or pages which expect form-type data) by selecting **Form Submission** as type, or submit custom data via a POST or PUT request by selecting **POST/PUT Data**. Consult the API documentation to determine which type will work correctly.
Load template
When submitting event data to a web service listed under templates, simply select the template and all required form fields will automatically be pre-loaded. User-specific fields (e.g. API keys) will need to be manually configured and are indicated with text enclosed in <>.

To suggest a new web service to be included in the list of templates, simply send us an email.

URL
The URL of the web page that contains the form to submit. This field supports variables.

Authentication
Authentication Method: Basic Authentication, Digest and NTLM are supported authentication methods. Username / Password: The authentication credentials.

It is recommended to only use basic authentication when submitting a form through a secure (https://....) web page.

Form Submission: Form Fields
Up to 20 form fields can be specified to be submitted. You can either include dynamic information by using one of the supported variables, or specify static information for the form fields.
The "Form Element Name" is the name of the form element, whereas "Value" refers to the contents of the form element value. Please see the Variables chapter for information as to which variables are supported.

POST/PUT Data
For APIs which expect POST or PUT requests, the content type, submission type (POST/PUT) and data need to be defined. The same variables which are supported in the Form Fields are supported in the data field as well.

Convert to UTF8: Converts dynamic data from variables (e.g. $EVENTSOURCE, $EVENTMESSAGE ...) to UTF8 before transmitting.

A typical POST/PUT setup is shown in the screenshot below:

GET
Submits a HTTP GET request to the specified URL. Data returned by the web page is available in event 642 logged if the HTTP(S) GET request was successful.

4.4.14.1 Troubleshooting HTTP
For form submissions, the HTTP does not download the web page containing the form prior to submitting it. As such, all necessary form fields will have to be specified in the list (e.g. input type="submit" type fields).

For example, HTML-based forms are sometimes submitted through a submit button (<input type="submit" name="NameOfButton" value="SomeValue">). If this is the case, then the name/value pair for the submit button ("NameOfButton"/"SomeValue" for the previous example) will need to be specified in the action.

This action logs the following events to the application event log with the EventSentry event source:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>640</td>
<td>Unable to submit the web-based form.</td>
</tr>
<tr>
<td>642</td>
<td>Action was triggered successfully.</td>
</tr>
</tbody>
</table>

4.4.15 Sound
EventSentry can play a wav file to indicate that an event has occurred. This sound file is played independently from the GUI which can also play a sound whenever an event occurs.
Filename
The filename of the wav file to be played. A sound card must be installed in the computer for this to work.

Test
Click the test button to play the sound file.

4.4.15.1 Troubleshooting Sounds
No troubleshooting information is available at this time.

4.4.16 Desktop
Forwards an event either to a local/remote instance of the management console or an instance of Growl.

Management Console
The receiving host will need to have the management console running and needs to be configured (Tools - Options - General) to either display a pop-up window or a balloon message. The management console can also be configured to play a WAV file.

Since the desktop action uses windows mailslots to send messages across the network which do not support encryption or authentication, it is recommended that you do not send security-sensitive information through this notification. You are also encouraged to verify security-sensitive messages received through the Desktop action from remote hosts, as they can be forged quite easily.

Growl
Forwards an event to a host running Growl. One or more variables can be used in the "Title" and "Message" fields, available variable names can be seen by clicking the arrow in the drop-down control. A password is only necessary if the host running Growl requires a password. "Use TCP" is recommend for most scenarios. **Allow network notifications** must be checked in the Growl Security dialog.

**Hostname**
Specify the host name where the messages are being sent to.

**Test**
Sends a test message.

### 4.4.16 Troubleshooting desktop notifications

Solutions for common problems with the Desktop action:

- The management applications needs to be active and correctly configured for this action to work properly. Please see the previous page for more information.

- Make sure that desktop notifications (either as a balloon or popup window) are activated in the General Options of the management application.

- Make sure that Growl is running and configured to accept network messages. When a password is configured, make sure the password matches.

This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>580</td>
<td>A mailslot could not be created.</td>
</tr>
<tr>
<td>581</td>
<td>Action &quot;%1&quot; was unable to send a notification to the (remote) Growl listener. Make sure the remote host is running Growl, accepting network messages, and no firewall is blocking traffic.</td>
</tr>
</tbody>
</table>

### 4.4.17 Network Message

Sends a network message, similar to the "msg.exe" command line utility, to a remote host using the Remote Desktop Services API. When "Use Remote Desktop Services" is unchecked, sends a message using the "Messenger" service.

The host sending the message must have permission to do so, see Prerequisites for more information.

If the host receiving the message is running Windows 2003 or later, then "Use Remote Desktop Services" should always be checked.
Host receiving the message. Remote host be running the "Messenger" service when "Use Remote Desktop Services" is unchecked.

**Test**
Click this button to send a test message to the remote host.

```
EVENTLOG: Security
EVENT TYPE: Audit Success
SOURCE: Microsoft-Windows-Security-Auditing
CATEGORY: Process Creation
EVENT ID: 4688
COMPUTER: BLACKJAGUAR
TIME: 10/19/2013 11:45:42 AM
MESSAGE:
A new process has been created.

Subject: Security ID: NT AUTHORITY\LOCAL SERVICE
        Account Name: LOCAL SERVICE
        Account Domain: NT AUTHORITY
        Logon ID: 0x3e5

Process Information:
        New Process ID: 0x2264
        New Process Name: C:\Windows\System32\auditlog.exe
        Token Elevation Type: TokenElevationTypeDefault (1)
        Creator Process ID: 0x418

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.
Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.
Type 2 is an elevated token with no
```

4.4.17.1 **Prerequisites**

When "Use Remote Desktop Services" is checked (default setting), it is important that the agent has permission to send the message to the remote host receiving the message. The account attempting to send the message needs the "Query Information" and "Message" permissions.
If the EventSentry agent is running under the LocalSystem account, then the computer account (e.g. SERVER05$) will require these permissions. If the EventSentry agent has been reconfigured to run under a specific user account, then that user account will require the “Query Information” and “Message” permissions.

Follow these instructions to authorize a user or computer account to send messages:

1. Log into the machine which should be receiving the messages
2. Open "Remote Desktop Session Host Configuration" under "Administrative Tools\Remote Desktop Services"
3. In the main pain, under "Connections", right-click “RDP-Tcp” and select “Properties”
4. Click the “Security” tab.
5. Click “Add”, and add the user or computer account to the list.
6. Make sure the user is selected in the user list and click “Advanced” on the bottom right.
7. Select the user account which was just added and click “Edit”.
8. Make sure that only “Query Information” and “Message” are set to “Allow”, as depicted in the screenshot.
9. Close all dialogs with "OK".
10. In most cases it is necessary to restart the machine where the permissions were made.

This action logs the following events to the application event log with the EventSentry event source in case of an error:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Problem / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>550</td>
<td>A net send message could not be sent.</td>
</tr>
</tbody>
</table>

4.4.18 Parallel Printer

EventSentry can print event log entries on a printer capable of interpreting ASCII characters sent to the parallel port. Most matrix printers on the market support that.

One example for printing event log entries is for audit failures of the security event log. Attach a matrix printer to a mission critical server and print audit failures to the matrix printer. In this case, even if an attacker manages to remotely clear the log files, no information is lost.

<table>
<thead>
<tr>
<th>Port</th>
<th>Supported are LPT1, LPT2 or LPT3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Length</td>
<td>If the printer is offline then EventSentry will buffer up to Buffer Length event log entries. The buffer size can between 256 and 32768.</td>
</tr>
</tbody>
</table>

To test if your printer will function properly simply attach it to the selected parallel port and hit Test. If the printer prints a test line then you will be able to use this printer.
4.4.18.1 Troubleshooting Parallel Printers

No troubleshooting information is available at this time.

4.5 Computer Groups

Computer groups allow you to categorize servers and workstations into groups so you can manage large amounts of servers and workstations more easily. EventSentry will need at least one group to function properly, and the local computer is always automatically added to the first available group if it does not exist in another group.

Group Types

There are three different kinds of groups that you can create in EventSentry:

- **Remote-Update Only Group**
  Manages remote EventSentry agents (e.g. install agents, update agents, etc.).

- **Heartbeat-Enabled Windows Group (default)**
  Manages remote agents (just like the Remote-Update Only Group) but also monitors the uptime and availability (hosts and agents).

- **Active-Directory Linked Group**
  Groups linked to Active Directory (AD) can either be a "Remote-Update Only" or a "Heartbeat-Enabled Windows" group, but group membership is directly linked to an OU or group in Active Directory (more information).

- **Heartbeat-Only Group**
  This group type is intended to be used to monitor hosts without the use of an agent through PING and TCP checks only. This group type is useful to monitor Unix-based computers, routers, printers, switches etc.

Managing Groups

**Adding a Group**

You can add a new group by right-clicking the "Computer Groups" and selecting "Add Group".

**Deleting a Group**

You can delete a group by right-clicking the group container and selecting "Delete". All information, including all package assignments will be permanently removed as soon as you save the configuration.

**Renaming a Group**

You can rename a group by right-clicking the group container and selecting "Rename" or by selecting the group and pressing the F2 button on your keyboard.

**Assigning Packages**

You can assign packages either to a group or a computer. To assign a package to a group, right-click the group and select "Assign Package(s)...". To assign a package to a computer, right-click the computer and select "Assign Package(s)...".
Adding Computers
You can add computers that are to be monitored either manually or import them using the import wizard. Click here for more information.

Setting additional authentication
If you cannot use your current credentials to manage remote computers then you can assign credentials with the authentication manager.

The user name and password you enter will be encrypted in the registry, and can only be decrypted by the user who encrypted them. For example, if Admin1 logs on to a computer and sets a username/password on a group or computer and Admin2 logs on to the same computer, then Admin2 will not be able to see the username and password entered by Admin1.

To remove previously set credentials, follow the same procedure but click on the “Remove Authentication” button instead.

If you intend to monitoring the EventSentry agent status on computers in a group where you set Authentication, then please read this note.

Managing EventSentry agents
You can use Remote Update to manage remote agents (install agents, updating agents, pushing the latest configuration etc.).

Using Variables
You can use variables throughout EventSentry to make the configuration and administration of the product easier. Variables are created and defined by right-clicking the Computer Groups container, and can be overwritten on a per-group level. Please see “Variables” for more information.

4.5.1 Adding Hosts
Computers can be added to a group in a number of ways:

- Manually
- Imported from a text file
- Imported from the Network Neighborhood
- Imported from a network scan
- Imported from Active Directory
- Linked to an Active Directory OU or group

Adding Computers individually
Right-click a group and select "Add Computer / IP Address ...". If EventSentry is configured to prompt you for an IP address when adding computers (Tools -> Options -> Remote Update) then you will be presented with the following dialog:
If you specify an IP address in the "IP Address (optional)" on this dialog, then EventSentry will add the host name to the group container, but always connect to the IP address of the remote host instead of connecting using the host name. If you rather work with IP addresses then you can also just enter the IP address in the "Computername / IP Address" field.

If EventSentry is not configured to prompt you for an IP address, then you will be prompted to enter the host name or IP address.

**Notes**
You may also enter notes for a computer which will be visible under "Inventory - Computer" in the web reports.

**Trusted Host**
Trusted hosts receive full action details (e.g. database connection string) even when an action is configured for enhanced security. A host should be configured as a trusted host when:

- A collector is enabled and in use
- An action is configured for enhanced security
- The host is either running the **Heartbeat** service, the **Network Services** service or any other EventSentry utility (e.g. Database Import, Purge Utility) which requires a full details of a specific action.

It is recommended that you do not use FQDN names when adding computers that are not joined to an Active Directory domain. Otherwise, problems with package assignments might occur.

**Importing**
To start the import process, right-click a group container and select "**Import Computers ...**".
This will start the **Import Wizard** as shown below. Select an **Import** type and click **Next**.

Click on the links below for more information on a particular import type:

- Import from a [Text File](#)
- Import from the [Network Neighborhood](#)
- Import from [Active Directory](#)
- Link to [Active Directory](#)

### 4.5.1.1 Import From Text File

You will be presented with the dialog shown below after selecting the **Import from File** import method:
Importing adds all computers specified in the import file to the current list of computers, the file should list one computer name per line. Existing computers are not removed from the list.

**Note:** If the import file does not contain group specifiers (see File Format in "Exporting") then all computers of the file are added to the currently selected group. If the file does contain group specifiers then only computers from matching groups will be imported.

After you have selected the file to import from click **Next** to see the summary screen:
4.5.1.2 Import From Network Neighborhood

You will be presented with the dialog shown below after selecting the **Import from Network** import method:
Choose a domain and then click on **Next** to select the individual computers:
Clicking on a computer name will either select or deselect the name in the list. To select all computers click the **Select All** button. When you are done click **Next** to see the summary screen as shown below. Click finish to start the import process.
4.5.1.3  Network Scan

Multiple hosts can quickly be imported from a network scan (discovery). A network scan is directed at a specific subnet and starts a multi-threaded scan of all available IP addresses in the address range specified.
Subnet
Specifies the subnet to scan in CIDR format.

TCP Port(s)
Allows the discovery of hosts which are not responding to ping (ICMP) requests but listening on a TCP port. By default, hosts are discovered through ping (ICMP) requests, but failing that can also be discovered using one or more TCP ports. When one or more TCP ports are configured, EventSentry will first attempt to ping the IP address and, if no response is received, attempt a TCP connection to the listed TCP ports. Multiple TCP ports need to be separated with a comma.

Listing one or more TCP ports will slow down the speed of the network scan.

MAC Vendor
When specified, only imports hosts where the manufacturer of the network card matches the specified string pattern (wildcards are supported). For example, to only import DELL devices, specify dell or *dell*. Note that MAC addresses which are not properly registered in the MAC vendor database will not be imported.

Resolve IP address
Resolves discovered IP addresses to a host name (recommended). Selecting this option will slightly reduce the scan speed.

Use FQDN
When resolving IP addresses, returns the host names in FQDN format.

4.5.1.4 Import From Active Directory

The Active Directory feature allows you to either import computers from Active Directory (by specifying an OU or group) or permanently link the group to Active Directory which retrieves the computers from Active Directory rather than storing them in EventSentry.

You will be presented with a dialog looking similar to the one shown below after selecting the Active Directory import method:
Select the container or Organizational Unit you would like to import computers from and click Next. You can also check the "Include Subcontainers/Groups" checkbox to include computers from subcontainers, or check the “Include disabled computers” box to also import disabled computers which are skipped by default.

After clicking Next you can view the computer names about to be imported and select or deselect individual computers:
To import all computers simply click **Select All**. Clicking **Next** again will show a summary screen:
4.5.1.5 Linking To Active Directory

If you have a working Active Directory infrastructure then you can link groups to Active Directory rather than importing the computers. This way you will only need to maintain the computers once, in Active Directory.

Every time you perform a remote update task in a linked group, the computer names are retrieved from Active Directory rather than from the local configuration. You may only link some groups to Active Directory, you are not required to link all groups to Active Directory.

To link a group to Active Directory, right-click the computers item in the desired group and select "Link to Active Directory". You can also select the "Link Group To Active Directory" checkbox when importing from Active Directory.

Remember that when the source OU or group in Active Directory change, EventSentry will not update the computers in the group automatically. You will need to perform a remote update action (e.g. Check Status) in order to trigger a refresh of the computer list.

After clicking Next in the wizard you will be presented with a dialog similar to the one shown below:
In the "Select Active Directory Container/Group" dialog, select the OU or group in Active Directory to link to. To view the tree of a different Active Directory domain, simply enter a path into the "Root Path" field and click the Refresh button.

When done click Next and you will be presented with the confirmation dialog:
Once a group is linked to Active Directory, you will not see any computers under the **computers** object. All remote update actions will be applied to all the computers of the Active Directory OU/Group you linked to.

**AutoSort**

You can right-click a group container and select **AutoSort** to have the computers retrieved from Active Directory automatically sorted alphabetically.

All existing computers of a remote update group will be removed when you link a group to Active Directory.

### 4.5.2 Deleting & Moving Hosts

**Deleting a single host**

Hosts can be deleted individually either by choosing "Delete" either from the right-click menu or the ribbon. When deleting a single host, the management console will issue prompt confirming whether the agent should be installed from the remote host (when deleting hosts from a group containing agents) or whether the host should just be removed from the management console.
Note that an agent can always be removed manually from a monitored host through the control panel, simply uninstall the "EventSentry Agent" application. Hosts cannot be removed from groups which are linked to Active Directory.

Deleting multiple hosts
Multiple hosts can be deleted through the remote update feature if the "Use Checkboxes" feature is enabled in the remote update options. To delete multiple hosts:

1. Ensure "Use Checkboxes" is enabled.
2. Select a group from which to delete multiple computers from.
3. Select "Check Status" either from the ribbon or by right-clicking the group.
4. Optional: In the resulting list, sort computers.
5. Check the hosts that should be deleted. Right-click the main area to clear/select all hosts, as well as toggle check boxes with the "Toggle Selection" menu option.
6. Right-click the main area and select "Deleted checked hosts" to delete the hosts from the group.
7. Verify the computers have been removed correctly and save the configuration.

Deleting hosts through this method will not uninstall remote agents.

Moving a single host
A single host can be moved by dragging the computer icon from one group to another.

Moving multiple hosts
Multiple hosts can be moved through the remote update feature if the "Use Checkboxes" feature is enabled in the remote update options. To move multiple hosts:

1. Ensure "Use Checkboxes" is enabled.
2. Select a group from which to move multiple computers from.
3. Select "Check Status" either from the ribbon or by right-clicking the group.
4. Optional: In the resulting list, sort computers.
5. Check the hosts that should be moved. Right-click the main area to clear/select all hosts, as well as toggle check boxes with the "Toggle Selection" menu option.
6. Right-click the main area, select "Move Checked Hosts To" and pick a group to which the hosts should be moved to.
7. Verify the computers have been moved correctly and save the configuration.
4.5.3 Authentication

Custom Windows, SSH and SNMP credentials can be managed by the Authentication Manager and

- set globally
- applied to a group
- applied to a computer

Apply custom credentials is necessary under the following conditions:

- The currently-logged on user does not have permission to install and/or update agents on remote hosts
- The user account under which the heartbeat agent is running does not have permission to query the EventSentry service status on remote hosts
- Remote hosts use SNMP v3 authentication or SNMP v1/v2c authentication with a community other than "public"
- Remote hosts support SSH

Credentials in the authentication manager are used by the management console when accessing remote hosts through remote update or the event viewer and by the Heartbeat Agent when polling the remote agent status or retrieving SNMP information. Since all credentials configured in the authentication manager are encrypted, it is required that the heartbeat agent service run under the the same Windows account under which the credentials are entered in the management console.

**Important Info for Windows Credentials & Heartbeat Monitoring**

Windows credentials entered will be encrypted in the registry, and can only be decrypted by the user who encrypted them. E.g., if user Bulls\DerrickR configures credentials for hosts, then the EventSentry Heartbeat Monitor service needs to also run under the Bulls\DerrickR user account.

Note that the Heartbeat Agent, when utilizing the collector, does not need to utilize Windows credentials.

The authentication manager is accessible via Tools -> Options, or by selecting

- computer groups
- any group
- any host

and clicking "Set Authentication" in the ribbon or the context menu.
Adding Accounts
EventSentry supports Windows, SSH and SNMP accounts, both of which are identified by a unique "Account Name" which identifies the credentials. The "Account Name" and the actual user name can be the same, but an account name must be unique. Account names are case sensitive. An account is added by clicking the + icon in the authentication manager.

Windows / SSH
Specify a valid user name, including the domain when necessary (Windows only), as well as a password.

EventSentry automatically determines whether to use Windows or SSH credentials depending on the group / host type.

LAPS Support
Windows credentials can be configured to use LAPS by checking the "Use LAPS" check box. LAPS is only utilized by the management console (for agent management), the heartbeat agent does not have the ability to dynamically retrieve LAPS passwords from AD.

SNMP
For SNMP v1 and v2c only a community needs to be specified.

For SNMP v3, a user name and either Authentication, Encryption or both Authentication and Encryption can be specified.

Assigning Credentials
Credentials can be assigned to the selected entity by either selecting an account name from the list or by adding a new account to the authentication manager with the + icon. A green check mark next to an account name indicates that the account is assigned to the currently selected entity.

Removing Credentials
Credentials can be removed from a selected entity by clicking "Set Authentication" in the ribbon or the context menu and subsequently clicking "Clear Selection" in the authentication manager.

4.5.4 Exporting Computers
Depending on whether you right-clicked a group or the Remote Update node, exporting will write either all computers from the selected group or from all groups to the specified text file.

Removing computers from the list
You can remove single computers, all computers from a group or all computers from all groups:

Single computer
Right-click a computer and click Delete or select a computer item and hit the Del button on the keyboard.

All computers from group
Right-click a group and select Delete All.
All computers from all groups:
Right-click the Remote Update node and select Delete All.

File Format
The text file used for imports and exports should be configured to the following format:

```
[Name of group]
computer1
computer2
computer3
[Name of next group]
computer10
computer11
[Another group]
computer70000
computer70001
```

Names in brackets describe the start of a new group whereas names alone specify computer names.
To see an example of such a text file simply add a couple of computers to the computer list and export it to a text file. You can then use this file as a template for future imports.

4.5.5 Variables
Variables allow you to create more flexible configurations when objects such as actions share most but not all configuration values.

EventSentry supports runtime and custom variables. Runtime variables are determined during runtime (e.g. $HOSTNAME, $LOG, etc.) whereas custom variables are defined by you.

Variable names are case sensitive and always start with the dollar $ character.

Defining Custom Variables
You define custom variables globally by right-clicking the "Groups" object and selecting "Define Variables". You will then be presented the Variables dialog:
Variables should be initialized with a default value which can then be overwritten on a per-group basis. Custom variables can be used in certain filter and action fields, please see "custom variables" for more information.

To change the default value of an already defined variable, double-click it. To remove already defined variables, select the variable and click "Delete".

Variable names will be referenced by prepending the dollar sign ($), as used in some programming languages. For example, to use the variable SMTPSERVER showed above in the SMTP Server field of a SMTP action, you will need to write $SMTPSERVER.

Overriding Default Values
You can override the default values of variable on a per-group or on a per-computer basis. In the example above, you can easily specify different SMTP servers for different groups, without having to create multiple SMTP actions.

To override variables, right-click the group or computer for which you would like to override the variable and select "Set Variable(s)". You will be presented with a similar dialog, though slightly different:
As you can see, the Add and Delete buttons are not present anymore as you can only define variables when right-clicking the “Groups” object. In a particular group, you can only change (=override) the values.

In the screen shot above the default value for the SMTPSERVER variable has been changed to mail2.netikus.net. The COMPANY variable however has not been changed, as indicated by the X in the Inherited column.

To override a variable double-click the name and enter a new variable value. Previously customized variables can be reset to their default value by simply clicking the “Inherit” button or by clearing the “Value” field.

4.5.5.1 Supported Variables and Fields

Run-time variables

Run-time variables are variables that may change during run-time or that depend on the event record being processed. These variables are supported in the following fields:

For email actions, event variables (e.g. $EVENTID) always reflect the value of the first event contained in the email (since emails may contain multiple records).
### Event Variables (1)

- $GROUP
- $FILTER
- $PACKAGE
- $NOTES
- $EVENTLOG
- $EVENTTYPE
- $EVENTSOURCE
- $EVENTCATEGORY
- $EVENTID
- $EVENTUSER
- $EVENTDATETIME
- $EVENTDATETIMEISO8601
- $EVENTNUMBER
- $EVENTCOMPUTER
- $EVENTMESSAGE

### Date / Time Variables (2)

- $DAY
- $MONTH
- $YEAR
- $HOUR
- $MINUTE

In email actions, the $LOG variable may be resolved to "Various" in the subject if the email contains events from multiple event logs.

<table>
<thead>
<tr>
<th>Email</th>
<th>File</th>
<th>Syslog</th>
<th>SNMP Trap</th>
<th>Desktop Trap (Growl)</th>
<th>Process Action</th>
<th>Event Log Backup</th>
<th>Service / Process</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender Name</td>
<td>Sender Email</td>
<td>Subject</td>
<td>Header &amp; Footer</td>
<td>Email Msg Override</td>
<td>File Name</td>
<td>Prefix</td>
<td>Custom Data</td>
<td>Title Message</td>
</tr>
<tr>
<td>$HOSTNAME</td>
<td>$HOSTNAMEFQDN</td>
<td>$HOSTNAMEALIAS</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$EVENT...VARIABLES (1)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$STR1...</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$STR28...variable</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DATE / TIME VARIABLES (2)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$LOG</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$COUNT</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$IPADDRESS</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>$LICENSEE</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

In email actions, the $LOG variable may be resolved to "Various" in the subject if the email contains events from multiple event logs.
$IPADDRESS: Resolves either to the IP address associated with a host entry in a group, or - if not set there, to the IP address of the interface with the fastest network connection on the system.

Insertion String Variables
Most Windows events are based on templates and contain dynamic values usually called "Insertion Strings" or "Event meta data". These insertion strings are exposed as variables in EventSentry and can be used in most actions.

Insertion string variables always start with $STR and are supported both in numerical (e.g. $STR2) as well as textual form (e.g. $STRIpAddress). The sequence number of an insertion string can be identified with the Event Message Browser, where insertion strings are identified with percentage signs followed by a number, e.g. %1, %2 etc..

Event insertion string are specified with the $STRx variable, where x is replaced with the number from the insertion string. For example, to display the 3rd insertion string from an event in an email subject, $STR3 could be included in the email subject of the action. The above table lists which fields support insertion string variables.

Insertion strings in their textual form are also specified using the $STRx variable, whereas x is replaced with the name of the meta data element. For example, $STRSubjectUserName would resolve to the content of the field SubjectUserName. Data element names can be found in the Windows event viewer in either the "Friendly View" or "XML View" tab of the event details tab.

Variable names are case sensitive - only $STRSubjectUserName would resolve to Administrator in the example below, $STRSUBJECTUSERNAME would not!
Custom Variables
Custom variables can have any name, but may only contain letters. Numbers and special characters are not supported in the name of a custom variable. Custom variables are supported in the following fields:

Backup Event Logs
Backup File ("File")

Log File Monitoring
File Path

Filters
Source
Category
Username
Computer
Advanced: Email Subject Override
Advanced: Email Content Override

SMTP Notification
Sender Name
Sender Email
Recipients
Subject
Primary (incl. User & Pass)
Secondary (incl. User & Pass)
Dial
Tags can be assigned to both groups and hosts and can be used to streamline package assignment as well as web-based reports. Tags are especially useful for larger installations where organizing hosts by groups only can be insufficient.

Consider the following scenario: Your environment consists of both production and development hosts, all of which are members of various groups (e.g. web servers, database servers, ...).

You cannot create a production and development group, because the hosts are already members of other groups. You want to assign different packages to the production hosts and also run reports that only return results for either production or development hosts.
By tagging hosts with their respective tags, the auto-assign package feature can be used to dynamically assign packages, while the “tag” keyword in the web reports can only return results from hosts that are tagged with the respective tag.

Hosts and groups can be tagged by selecting the "Assign Tags" option from either the context menu or the ribbon. The tag icon in the ribbon is context sensitive and will show in blue if the currently selected group or host has one or more tags assigned, and will be shown in gray otherwise.

Tags set on a group-level are automatically inherited by all hosts which are a member of that group, it is not possible to block tag inheritance. Multiple tags can be assigned to both groups and hosts.

Once a host or group is tagged it can be used to automatically assign a package or filter any search-based web reports page using the `tag:` keyword.
Editing tags for multiple hosts
Tags can be edited on multiple hosts via the Remote Update feature's context menu. To edit a tag on more than one host do the following;

1. Select “Computer Groups” or a specific group
2. Select “Check Status” from the ribbon or context menu
3. Check/uncheck the hosts on which you want to edit tags on the right pane
4. Right-click anywhere and select “Edit Tags”
5. Add or remove tags and click OK

Note: When editing tags on hosts that have different tags assigned already, then the specified tags will be added to the existing tags of each checked host. Existing tags will not be affected.

4.6 Managing Agents

Remote Update helps you deploy and manage the EventSentry agent on remote hosts as well as verify connectivity with network devices. The agent configuration as well agent patches can also be managed by the collector.

Remote Update has the following capabilities divided into three categories:

Check Status
- Performs a connectivity test based on the heartbeat settings of the group (or host), also checks the agent status when processing Windows hosts.

Check Agent Status
- Retrieves the current agent status and installed version from a number of hosts to help you make sure that the EventSentry agent is running and has the latest version. Only adds full hosts to the list when selected from the “Computer Groups” context.

Update Configuration
- Pushes the current configuration to the remote host(s)

Perform Action
- Install the service (including necessary files)
- Update the service executable on remote computers
- Uninstall the service (including files and configuration)
- Start the service on remote computers
Stop the service on remote computers

Requirements
The remote update tasks have different requirements, depending on which action is performed. The table below shows you which tasks have which requirements.

<table>
<thead>
<tr>
<th>Remote Update Task</th>
<th>Remote Registry</th>
<th>ADMIN$</th>
<th>ESS</th>
<th>Service Control Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Service</td>
<td>optional, to set automatic service restart option</td>
<td>yes, to copy service file and initial configuration</td>
<td>if the RemoteUpdate sub directory exists</td>
<td>yes, to install service</td>
</tr>
<tr>
<td>Uninstall Service</td>
<td>yes, to remove config</td>
<td>yes, to remove service file</td>
<td>no</td>
<td>yes, to uninstall service</td>
</tr>
<tr>
<td>Update Configuration</td>
<td>no</td>
<td>yes, if ES$ not present</td>
<td>if the RemoteUpdate sub directory exists</td>
<td>no</td>
</tr>
<tr>
<td>Update Configuration (with &quot;minimize traffic&quot; activated)</td>
<td>no</td>
<td>optional, to query version of remote agent</td>
<td>if the RemoteUpdate sub directory exists</td>
<td>no</td>
</tr>
<tr>
<td>Check Agent Status</td>
<td>no</td>
<td>yes, to query version of remote agent</td>
<td>no</td>
<td>yes, to query the current service status</td>
</tr>
<tr>
<td>Update Agent</td>
<td>no</td>
<td>yes, to update service file</td>
<td>if the RemoteUpdate sub directory exists</td>
<td>yes, to stop and start service</td>
</tr>
</tbody>
</table>

For example, to update the configuration on a remote host, the remote host either needs to have the ADMIN$ share or the ES$ share present. To install the service remotely, the ADMIN$ share is mandatory and access to the service control manager is also required.

To perform a Remote Update:

1. Make sure that the service files (eventsentry_svc_x64.exe, eventsentry_svc_x64.exe) are accessible on the Management Computer.

2. Add all the computers that you would like to update to the Computer list. If you would like to add computers from a text file, the network neighborhood or Active Directory then right-click a group and choose Import. Please see the next page for details on importing computers. You will not be
able to add the local computer name into this list since it is assumed to already be up-to-date and to serve as the template.

3. Right-click a group or right-click **Groups**. The former will only update computers in the selected group while the latter will update all computers from all groups.

4. Choose the desired category from the context menu

5. Click on a category for more details:
   - **Retrieving Service Status** ("Get Status")
   - **Performing Updates** ("Update Configuration")
   - **Managing Agents** ("Manage Agent(s)")

6. If you selected **Use checkboxes** then you will now need to check the computers to which the update should be applied to. Then right-click the list and choose **Go** from the context menu or click the green arrow in the toolbar.
Saving the results
You can always save the results of any remote update status / update / action by right-clicking the list and selecting Save List As.

This will save the current output in a text file.

Repeating an update
If you would like to repeat any status / update / action then right-click the list and select Repeat Update. The last action you performed will repeated.

Note: If you activated the Use Checkboxes feature then you will need to click on Go instead of Repeat Update.
4.6.1 **Options**

You can customize the remote update feature and configure several options by navigating to **Tools -> Options -> Remote Update**. For example, you can optimize the remote update process for WAN networks, ping hosts before a remote update is performed and much more.

Please see **Management Console -> Customizing -> Remote Update** for more information.

4.6.2 **Authentication**

By default, when using the remote update, EventSentry connects to remote computers with the user name you are currently logged on as. This might prove difficult when you have to administer different domains and/or servers that require you to authenticate as a different user.

If you would like EventSentry to use different credentials when connecting to remote machines then you can do one of the following:

- Specify credentials globally
- Specify credentials per group
- Specify credentials per machine

Credentials set on a per-machine level will override credentials set on a per-group or global level, credentials set on the group level override global credentials.

![Alert symbol] If you intend on monitoring the EventSentry agent status on computers in a group where you set Authentication, using the Heartbeat Agent, then please read this note.

**Specifying global authentication credentials**

Different credentials can be set on a global level, to affect all configured computers. To set global credentials, right-click the **Computer Groups** container and select **Set Authentication**. Global credentials affect all computers, unless other credentials are set on a per-group or per-host level.

**Specifying different Credentials per group**

You can set a different user name/password by right-clicking the group icon and selecting **Set Authentication** as shown below.
This will bring up a dialog where you can enter alternate credentials:
Once username and password are set EventSentry will use these credentials when connecting to any computer in that particular group. This includes directly connecting to computers with the Connect feature when right-clicking computer items.

The username and password you enter will be encrypted in the registry, and can only be decrypted by the user who encrypted them. For example, if Admin1 logs on to a computer and sets a username/password on a group or computer and Admin2 logs on to the same computer, then Admin1 will not be able to see the username and password entered by Admin2.

**Specifying different Credentials per Machine**

When only a few machines need different credentials then you can set a username and password on a per machine basis. This time right-click the machine name instead of the group.
and again select **Set Authentication**. Please note that credentials set on a per computer basis always override credentials set on a per group basis.

**Removing Credentials**
To remove previously set credentials again (whether for a group or for a computer) right-click the respective icon and select **Set Authentication**. In the dialog box click on **Remove Authentication** to have the credentials erased.

**Icons**
When you set different credentials for computer items or groups, then you will notice that the icon shown in the tree pane will have a little green card added to it as shown in the figure below:

This is to indicate that different credentials are stored, in the example above on **TEST18-W2K16**.

### 4.6.3 Check Status
A typical status check will look like this:

The service status report shows you the following information:
• **Whether the EventSentry service is installed or not**
  This information is visible in the *Status / Result* column of the output.

• **The status of the service (running or stopped)**
  This information is visible in the *Status / Result* column of the output.

• **The version of the service**
  This information is visible in the *Version* column. If the service is not installed then the version number will be 0.00. Please note that the service version information is only accurate if the service is running.

To show the network-related columns (SNMP, Ping, TCP, ...) right click the results window and check the “Extensive Network Check” option. Enabling this option will perform additional network connectivity checks when processing Windows hosts. This option is the default when processing network devices.

• **The computer type of the remote machine (workstation or server)**
  The icon next to the computer name shows you whether the remote computer is running a workstation OS or a server OS.

  ![Workstation OS](image1)
  ![Server OS](image2)

  In addition to the OS type, the icon will show you additional information about the status of the remote computer:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Workstation or Server</th>
<th>EventSentry Agent Status</th>
<th>Network Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3" alt="Unknown" /></td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Initial icon, before “Remote Update” attempts to perform requested action</td>
</tr>
<tr>
<td><img src="image4" alt="Unknown" /></td>
<td>Unknown</td>
<td>Unknown</td>
<td>Down</td>
<td>Shown when the remote host is not reachable (e.g. not responding to ping)</td>
</tr>
<tr>
<td><img src="image5" alt="Server" /></td>
<td>Running</td>
<td>Up</td>
<td></td>
<td>Shown when the remote host is running a server OS and the agent is running</td>
</tr>
<tr>
<td><img src="image6" alt="Server" /></td>
<td>Stopped or not installed</td>
<td>Up</td>
<td></td>
<td>Shown when the remote agent is stopped, not installed, or a remote update error occurred.</td>
</tr>
<tr>
<td><img src="image7" alt="Workstation" /></td>
<td>Running</td>
<td>Up</td>
<td></td>
<td>Shown when the remote host is running a client OS and the agent is running</td>
</tr>
<tr>
<td><img src="image8" alt="Workstation" /></td>
<td>Stopped or not installed</td>
<td>Up</td>
<td></td>
<td>Shown when the remote agent is stopped, not installed, or a remote update error occurred</td>
</tr>
</tbody>
</table>

### 4.6.4 Pushing the Configuration

With the **Push Configuration** feature you can send the local configuration to remote hosts to avoid setting up multiple hosts manually with the same configuration.

The following settings are updated on remote hosts when you do a **Push Configuration**:
• Global Options
• Event Log, Log File, System Health and Security & Compliance packages
• Actions

Requirements
In order for EventSentry to transfer the configuration to the remote host, either the **ADMIN$** or the **ES$** share need to exist. Please see below for more information:

**ADMIN$**: This is the default administrative share which is activated on all Windows computers and shares the %SYSTEMROOT% directory (e.g. C:\Windows) to users of the Administrators group. If this share is present on your hosts monitored by EventSentry, then remote update will work flawlessly.

**ES$**: If, for whatever the reason, the **ADMIN$** shares are not present on your monitored hosts, then you will need to create the **ES$** share manually.

Instructions are as follows:
1. Create the directory `C:\Program Files\EventSentry\RemoteUpdate`
2. Share this directory as **ES$**. This will create a hidden share that is not visible to somebody browsing the network.
3. Only allow members of the **Domain Admins** or local **Administrators** write access to this share.
4. Restart the EventSentry agent(s).

Starting the Update
After you click the **OK** button you will see a screen similar to the one below where the configuration on the host **TEST17-W2K8R2** has been updated.

The screen shot above shows that Remote Update could not connect to the computer TEST1 (it was not turned on) and that the computer TEST17-W2K8R2 received the configuration update successfully. The TEST18-W2K16 computer was skipped because it is the EventSentry mangement server (local host) and does not require a Push Configuration - each time you click Save the configuration is updated on the EventSentry management server.

As with every remote update feature you can right-click the list and save the results in a text file.

Exclusions
The following features are excluded from the remote update feature and need to managed individually:

• Environment Settings (e.g. temperature settings, humidity settings etc.)
• All settings under "**Network Services**"

In order to manage the above settings, copy the management console (**eventsentry_gui_x64.exe** on 64-bit systems, **eventsentry_gui.exe** on 32-bit systems) to the remote host and run the management console there. These settings will not be overwritten by the next configuration update, whether initiated manually or through the collector.

### 4.6.5 Manage Agents

With the **Manage Agents** feature you can control and modify the EventSentry status on remote computers. The following actions can be performed:
- **Install** the service (includes copying necessary files) by deploying the agent
- **Update** the service executable on remote computers (restarts the service if necessary)
- **Uninstall** the service (including files and configuration)
- **Start** the service on remote computers
- **Stop** the service on remote computers

To perform actions on agents, select a **computer group** and use the toolbar to click **Deploy Agent**, or use the toolbar to click **Other Actions** and select an action such as **Upgrade/Update** from the drop-down menu. You can also right-click a computer group and select actions from the “**Manage Agent(s)**” menu:

![Toolbar actions](image)

After you choose the desired action (e.g. **Upgrade**) click the **GO** button in the toolbar to perform the action. You will see a screen output similar to the one shown below:

<table>
<thead>
<tr>
<th>Host</th>
<th>Action: Deploy Agent</th>
<th>Agent</th>
<th>Config Revision</th>
<th>SNMP</th>
<th>Ping</th>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEST17-W2K12R2</td>
<td>Agent updated successfully</td>
<td>4.0.12</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.6.6 Deploying Agents

If you want to setup EventSentry on a newly setup computer, that is a computer that does not yet have EventSentry installed, then you can use the “**Deploy Agent**” feature.

Simply add the host to a computer group, right-click the host and select “**Deploy Agent**”: 
Remote Update will automatically copy the EventSentry files, create the service, copy all configuration data (event log filters, system health, actions, ...) and start the service. You can deploy the agent to multiple hosts at the same time by selecting a computer group and then using the toolbar to click the **Deploy Agent** button and then click the **Go** button.

This feature is the quickest way to monitor a new computer with EventSentry.

**ODBC Drivers**

The EventSentry agent will automatically install PostgreSQL when those drivers are required (that is, at least one action uses a PostgreSQL database). The driver MSI files are distributed by the management console during a remote agent installation (if needed) and then later installed by the agent.

> **i** ODBC drivers are not required when using actions that utilize the collector.

### 4.6.7 Automating Remote Update

Remote update and the auto-deployment features of the collector make it easy to manage EventSentry agents since you are not required to install the software on the remote hosts manually. However in some cases, e.g. when you are not able to utilize the collector and need to manage a large number of hosts, utilizing the remote update utility may be necessary.

EventSentry includes a command-line version of the Remote Update feature (eventsentry_upd.exe) which you can schedule to run automatically at desired intervals using the Windows Scheduler (e.g. once a day). The EventSentry Remote Update Utility offers the following features:

- Push the configuration to remote hosts
- Only run when the configuration has changed
- Log summary information to the event log
- Automatically update remote computers to use the latest agent
- Automatically install the agent on a remote host if it is not already installed
• Automatically start the agent on a remote host if it is stopped

We recommend that you schedule the Remote Update Utility to run one or more times during the day (e.g. at night and in the morning), but you can also run it manually from the command-line. The Remote Update Utility consists of one file (eventsentry_upd.exe) and is installed into the EventSentry installation folder and supports the following command-line switches:

Scope
(required)
/allgroups Update computers in all groups.
/group:GROUP NAME Update computers in the specified group.

Options
/log Log results to the event log (details)
/installupdate Ensures that:
• The remote agent is updated to the latest version if it is out-of-date
• The EventSentry agent is installed if it isn't already
• The EventSentry agent is started if it is stopped
/repeatfailed If a host is unreachable, remote update will store the host name in a temporary file and attempt to contact the host again when the utility is called the next time and the configuration has not changed in the meantime.
/usead Use Active Directory: If you have ActiveDirectory-Enabled groups (more info), then you should activate this option. Remote Update will refresh the computer list from Active Directory and install the agent on computers that have been added to an OU or group.
/noping Do not ping remote hosts before attempting to an update
/uninstall Uninstall the EventSentry agent from remote hosts
(force Force a configuration update even if the local configuration has not changed

Examples
Simply running eventsentry_upd.exe with a scope option (e.g. /allgroups) will push the latest configuration out to all hosts, but you can leverage the utility more by using some of the command-line options.

Example 1: Pushing the configuration to all hosts
eventsentry_upd.exe /allgroups

Example 2: Pushing the configuration to all hosts in the “Servers” group, logging the result:
eventsentry_upd.exe /group:Servers /log

Example 3: Pushing the configuration to all hosts, logging the result and also ensuring that the agents are up-to-date and running:
eventsentry_upd.exe /allgroups /log /installupdate

Example 4: Pushing the configuration to all hosts, logging the result, refreshing the computer list from ActiveDirectory and installing the agent on newly added computers:
eventsentry_upd.exe /allgroups /log /installupdate /usead

The screenshot below shows the output of running the Remote Update Utility:
4.6.7.1 Return Codes & Event Log

Events logged by the remote update utility:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1100</td>
<td>The EventSentry Remote Update Utility has completed successfully.</td>
<td>The EventSentry Remote Update Utility has completed, 4 host(s) were updated successfully.</td>
</tr>
<tr>
<td>1101</td>
<td>The EventSentry Remote Update Utility has completed, but some hosts could not be updated.</td>
<td>The EventSentry Remote Update Utility has completed. 4 host(s) were updated successfully, 1 host(s) failed. The following hosts could not be updated: DC2-W2K.</td>
</tr>
</tbody>
</table>

Event ID 1101 is logged as a **Warning** when at least one computer could be reached an updated, otherwise it is logged as an **Error**.

Return codes (%ERRORLEVEL%):

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No errors, all hosts were updated successfully</td>
</tr>
<tr>
<td>3</td>
<td>Error reading the configuration</td>
</tr>
<tr>
<td>7</td>
<td>Invalid command-line options provided</td>
</tr>
<tr>
<td>9</td>
<td>The configuration update file (.reg) could not be created</td>
</tr>
<tr>
<td>10</td>
<td>One or more hosts could not be processed successfully</td>
</tr>
<tr>
<td>11</td>
<td>One or more hosts could not be processed successfully while repeating previously failed hosts</td>
</tr>
</tbody>
</table>

4.6.8 Remote Administration

It is **not recommended** that you manage a remote installation by connecting to it, instead we recommend that you manage all remote agents with **Remote Update**. If possible, only use the “Connect To” feature to review the active configuration on a remote host, not to manage it.

You can remotely administer any EventSentry installation just like a local one. The only setting that cannot be remotely administered is the **Remote Update** itself.

**Criteria:**

- You have permission to access the registry of the remote computer (on Win2k and higher please make sure that the **remote registry service** is running)
- You have read/write permissions to the registry key **HKLM\Software\netikus.net\EventSentry**
- The default administrative share `ADMIN$` exists on the remote computer (only necessary for remote service installation)

**Instructions:**

Option 1: Right-Click the local computer object and select **“Connect to remote host”**. You can also connect to a remote host by selecting a host within a computer group and then and clicking the “Connect Now” button in the toolbar.

If you chose “Connect to remote host”, it will prompt you to type in the computer name and click on “Connect Anyway”.

Remote Update features will not be available while you are connected to a remote machine. You will need to be connected to the local machine in order to perform a Remote Update.
4.7 Scripts

Scripts allow you to embed scripts of any kind (command line scripts, visual basic scripts, Perl scripts, etc.) inside the EventSentry configuration, so that the scripts themselves do not have to be maintained on the target machines, making it easier to maintain environments that utilize scripts.

Scripts can be utilized from these components:

- Application Scheduler
- Process action
- Validation Scripts

Scripts can be written in any language as long as the script interpreter (e.g. Perl) is properly installed on the machine where the script is going to be executed. For example, ActivePerl needs to be installed on a host where Perl scripts are configured to run.

Scripts are stored in the registry and can be configured in the sub nodes under the main Scripts node where the general options are configured.

User (Embedded)
User-maintained (embedded) scripts can be managed here, and clicking this node will display all existing user scripts.

Managed
Downloaded scripts maintained by NETIKUS.NET are shown here, and clicking this node will display all managed scripts. While managed scripts cannot be edited or deleted, they can be disabled and the execution frequency can be adjusted as well. Tags associated with scripts cannot be removed, but additional tags can be added.

Tags
Scripts can be tagged (and all managed scripts have at least one tag), which can be utilized in Validation Scripts packages.

Using Scripts
To use a script, prefix the file name with the @ symbol in an application schedule or process action. For example, if your script is named LaunchUpload.cmd, then specify @LaunchUpload.cmd. Fields that support embedded scripts feature a pull-down menu that lets you select from any of the configured scripts.
4.7.1 **General**

General Options apply to all scripts, whether user, managed, on-demand or validation scripts.

**Managed Scripts**

Managed scripts are maintained & updated on a regular basis, updates are available to evaluation users and customers with active maintenance agreements. Users can supplement managed scripts with their own, but managed scripts cannot be modified.

**Launch Folder**

This is the directory where the scripts will reside on disk and executed from. The default setting is % SYSTEMROOT%\system32\eventsentry.scripts, and can be customized by changing the Launch Folder.

Embedded scripts that are assigned to a particular host will be created in the launch folder of that computer when the agent is started. If a script is not assigned, meaning that is neither used by an application schedule, process action or validation scripts package, then it will not be created in the file system. Scripts in the launch folder will be deleted when the agent is stopped.

**Restrict Permissions**

The launch folder inherits its permissions from the parent folder by default, which will differ depending on the OS. To ensure that only the agent has access to the script files in the launch folder, you can check the Restrict Permissions check box. This will ensure that only the account the EventSentry service is running under (LocalSystem by default) will have (NTFS) permission to access the file(s).

4.7.2 **User & Managed Scripts**

Clicking on either “User (Embedded)” or "Managed" scripts will show a list of available user or managed scripts.

Managed Scripts are read-only, scripts cannot be added, edited or deleted. Only User (Embedded) scripts can be added, deleted or edited.

**Adding**

To create a new script, first navigate to Scripts -> User (Embedded) and then click the Add button from the ribbon. The name of the script is important, as this will be the name of the file in the launch folder. It is recommended that you specify a valid file extension (required when no interpreter is specified).

You can specify the script content in the Script Content text area, which supports scripts with up to 16384 characters. Scripts can either be edited in the script content field directly, pasted from the clipboard (paste button) or loaded from a file (Load button).

**Managing**

To edit an existing script, navigate to Scripts -> User (Embedded), locate the script to edit and double-click it. In the resulting dialog you can either edit the actual script directly in the Script Content text area, copy & paste the content to/from the clipboard or load/save the script to/from a file. Other properties, including the interpreter and tags can also be edited here.

**Deleting**

To delete a script, navigate to Scripts -> User (Embedded), select the script and click the Delete button in the ribbon. Keep in mind that any application schedules and/or process actions referencing the deleted script will no longer work when the script does no longer exist.
Type, On-Demand vs Validation

All scripts, either User or Managed, can either be on-demand or validation scripts. The vast majority of managed scripts are validation.

On Demand: Are referenced by either an application schedule or process action.
Validation: Are referenced by one or more validation scripts packages.

Enabled (Validation scripts only)

Enables or disables a script. This is mostly useful to disable managed scripts that are automatically included based on their tag as part of a validation script package, but should not be executed.

Interpreter
An interpreter is only necessary when the file extension that is used for the file cannot be mapped to an executable by the OS. For example, if you are adding a PERL script, then you can specify `perl.exe` as the script interpreter.

**Frequency**
Controls how frequently the script is executed, only available for validation scripts. The frequency of on-demand scripts is either controlled by the application scheduler or by events triggering the action. Validation script will follow this schedule, even when the agent is restarted or a new configuration is received. **Note:** If an assigned validation script is updated and pushed to the agent, it will be executed immediately, regardless of its schedule.

**Evaluation**
Validation Script packages determine whether a script passes or fails its test based on the evaluation criteria, which can either be its Errorlevel, a wildcard check or a RegEx check.

- **Errorlevel:** An `%ERRORLEVEL%` (return code) of zero indicates that a script passed its check, return code 999 indicates that the script is not applicable on the system and should be ignored. Any other error level indicates failure.
- **Wildcard:** Applies the specified wild card pattern to the output of the script. If the pattern matches, the script will pass its check.
- **RegEx:** Applies the specified RegEx pattern to the output of the script. If the pattern matches, the script will pass its check.

**Tags**
Can be specified for both On-Demand and Validation scripts, but are generally intended to be utilized by Validation Scripts packages for assignment purposes. For example, you can assign all validation scripts tagged `nist-800-53` to hosts that need to be NIST compliant. Tags associated with managed scripts cannot be removed, but additional user-defined tags can be added.

### 4.8 Internationalization

EventSentry can be used in environments that do not use English as the primary language and character set, including but not limited to Japanese, Korean and more. While the management console itself is only available in English, most notifications (e.g. email, file, database) do support foreign character sets and encodings.

**Management Console**
The management console is only available in English, but will display foreign characters correctly in the dialogs and built-in event log viewer. Foreign characters can also be used to configure EventSentry, for example in filter fields.

**Web Reporting**
Several translations exist (e.g. French, Japanese) for the web reports, and the language can be set using the Profile Editor. If you select one of the supported languages (please see Web Reports for more information on available translations), then the character encoding of the web reports will be automatically set. If a translation for your language does not exist or the automatic encoding type is incorrect, then you can set the encoding using the `profile editor` in the Localization section.

**Email and File Actions**
When configuring your email or file notification to use HTML, then EventSentry tries to automatically detect the correct encoding. If the encoding is not detected correctly or you want to manually set it, then you can change it by clicking the **Encoding** button in the “Internationalization Options” section. On the resulting dialog, clear the “Auto-Detect Language Settings” check box and specify the encoding in the **Character Encoding** field.
Database - ODBC Actions

No additional configuration steps are necessary when using a database action, however you will need to make sure that your database supports your locale. In Microsoft SQL Server®, make sure you select the correct collation mode when creating a new database, which means that you will have to create an empty EventSentry database prior to running the EventSentry setup or configuration assistant. No special settings are required for the built-in PostgreSQL database.

Please see the following two KB articles to avoid known problems when using languages that are not Latin-based:

KB-111
KB-112
KB-333
5 Monitoring with EventSentry

Overview
EventSentry is configured with the **EventSentry Management Console** application. The main interface is divided into two parts: the **tree pane** on the left and the **details pane** on the right.

The tree pane shows all objects organized by type while the details pane shows all details regarding a selected object:

Right-Click
Right-click items located in the left tree pane to modify them. For example, to add a new filter you right-click the group where you would like to add the filter.

This works the same way for all objects, including actions and computer objects.

Left-Click
To view the details of an object located in the left tree pane you left-click or double-click it (see usability for this setting). The object details (such as action details) will then be loaded into the details pane and the active object in the left pane will become bold as seen below:
Menu
In addition to the main interface, you can customize the behavior of the EventSentry management console application through the ribbon, where you can:

- Adjust **confirmation messages** to enable or disable confirmation dialogs (e.g., before a filter is permanently deleted)
- Adjust **remote update** settings
- Send feedback, suggestions, or bugs directly to us
- Visit our resources on the web

This agent does not need to be restarted when configuration changes are being made, including changes done through remote update.

5.1 Service Control

You can use the Services menu to manage the EventSentry agent, and other EventSentry services. The **Agent** section supports the following controls:

- **Start**: Start the service
- **Stop**: Stop the service
- **Restart**: Restart the service
- **Install**: Manually install the service
- **Uninstall**: Manually uninstall the service
- **Startup Type**: Switch the service startup type from Automatic to Manual and vice versa
- **Update**: Update the service executable
- **Debug Level**: Change the agent diagnostic logging level.
  
  **Recommended value: High**
- **View**: View the agent diagnostic log now.
The check boxes Files/Service indicate whether the necessary files and the service are properly installed.

**Agent**

The "EventSentry" service is the main service monitoring the event log, services, disk space etc..

It is not possible to manage the agent on remote computers using the Services menu. Instead, use the "Groups" tab of the toolbar to manage agents on remote computers.

For more information, see the [Managing Agents](#) chapter.

**Heartbeat Monitor**

The “EventSentry Heartbeat Monitor” service is used to monitor remote hosts and remote Event Log Agents.

**Debugging & Testing**

To verify if the service is operating correctly you can press the Create Test Events button. This will create three event log records that should be detected by the service as long as you are monitoring the Application event log and Information, Warning or Error event records.

The Current Version shows the version of the service as it was reported by the service when it was started the last time.

**Debug Level**

The EventSentry agent writes status messages to the event log and/or to a log file (%SYSTEMROOT%\eventsentry\logs\eventsentry_svc_X.log) upon request. It is recommended to use level "High" in case you experience problems with the service. The default max size for log files is 64MB but can be customized in the registry.

5.2 Global Options

The Global Options are settings that apply to all computers, regardless of their group membership. The global options are divided into the “General” and the “Heartbeat” settings, click the respective tab to access them.

**Boot Time Behavior**
EventSentry monitors the event log when it is running. When the service is not running (such as when the system is being rebooted), it is unable to monitor the event logs. Event log entries created while the service is stopped are not processed.

To avoid this problem you can configure EventSentry to look for events created after the service was last shut down by setting this feature to "most". Every time the service starts it scans the event log from the last checkpoint. This feature is also useful in determining if a server was rebooted.

**Most**: EventSentry will re-scan the event log and process events that occurred while the service was stopped.

**Regular**: EventSentry will monitor the event log right after the service was started, but will not process events that occurred while the service was stopped.

**Least**: EventSentry will ignore events that occurred for the first X seconds after the OS booted. For example, if EventSentry emails you a lot of events when a server is rebooted, then you can configure this feature to suppress events for a given amount of seconds. Click the “Settings” button to bring up the “Boot Delay Settings” dialog that lets you configure the interval and to which action types this feature applies to.

Note: SMTP emails sent from a boot scan will have "[RESCAN]" appended to the subject.

**Naming Schema**

This option controls how hosts identify themselves in the web reports.

**NetBIOS**
By default, computer names will appear with their NetBIOS names (e.g. SERVER1) in alerts and the web reporting.

**FQDN**
Hosts will show up with their respective FQDN names instead (e.g. server1.yourdomain.local) of just the host name. Please note that you will have to restart the agent for this change to become effective.

**Alias**
Forces hosts to show up with the name defined in the management console instead of their actual host name. This setting requires that at least one active IP address matches the IP address configured for the host name in an EventSentry group. This setting is useful for environments where hosts with identical names but from different subnets connect to the same EventSentry database. When configured, also supports the $HOSTNAMEALIAS variable.

It is not recommended to use the FQDN option when managing computers that are not part of an Active Directory domain, due to potential problems with the assignment of packages to those computers.
Certain action types, including email, database and Syslog, have the ability to cache events when the configured server is temporarily unavailable. This setting allows you to configure the maximum amount of disk space that EventSentry will use in the system temp directory (%TEMP%) for caching events.

This setting also applies to the storage used for the summary actions.

**Maximum Notification Intervals**

Many features, including environment monitoring, disk space and service monitoring write alert messages to the event log when a certain problem (e.g. low disk space, high environment temperature, etc.) is detected. To avoid the event log from being flooded with the same event pertaining to the same problem you can set a maximum notification interval here.

For example, if you set a maximum notification interval of 24 hours then a low disk space warning regarding drive C will only be logged once every 24 hours until the low disk space problem is resolved.

**Alert Clear Severity**

By default, performance & disk space monitoring features log events with the same event severity (as configured in the object) regardless of whether an issue has been detected or resolved. This is so that default event log filter rules process both alert & resolution identically.

Since this can both be confusing (an issue is resolved but logged as an “Error”), this setting overrides the default behavior and will log events that indicate that an issue has been resolved with the selected severity.

This setting only affects Performance Monitoring & Disk Space Monitoring.

**UTC Support**

Starting with version 3.0, EventSentry can write all time stamps in the UTC time zone to the database. This is helpful for networks spanning multiple timezones, since the web reports can display all data in the local time zone of the currently logged on user.

UTC support is enabled by default for new installations, and can also be switched on for users upgrading from earlier installations. Once enabled, UTC support cannot be turned off again.

UTC only affects the web reports, alerts generated by the agents for example still use the time stamp from the local time zone the agent is located in.

Review [KB article #240](#) when enabling UTC support after upgrading from 2.93.1 or earlier.

**Maintenance Schedules for Agents**
When maintenance schedules are created for a group or host, they only apply to heartbeat alerts generated by the Heartbeat Agent; any alerts (e.g. event log alert via email) are still sent out by an agent.

To suppress all email alerts during a maintenance schedule, check the "All email actions" check box; check the "All pager actions" check box to suppress all pager alerts.

Both check boxes are checked by default with new installations.

Security Options

Agents: only store the group agent is a member of in local registry config
By default all remote agents receive the full EventSentry configuration transmitted, including all groups and hostnames contained therein. This may not be desirable in situations where the same EventSentry configuration is used to monitor disparate & isolated networks, such as in MSP environments. Enabling this option ensures that a remote agent only stores the group data from the group it is a member of.

Geolocation

EventSentry ships with a free Geolite city geolocation database which will supplement IP addresses with their corresponding geolocation. EventSentry includes this database, which is updated with every EventSentry version update that is released. The latest version of the database can also be downloaded from http://dev.maxmind.com/geoip/geoip2/geolite2/. Follow the steps below to update the geoip database:

1. In the management console, click on "Services"
2. Stop the "Network Services" service
3. Stop the "Collector" service if it is running
4. Replace the GeoIP database file with the latest version (mmdb format only!)
5. Start the "Collector" service again if it was running
6. Start the "Network Services" service

Get Threat Intel

Utilizes three public black lists (OTX, Firehol, Blocklist.de) that are downloaded every 4 hours to identify potentially malicious IP addresses. If an API key is configured, then a black list from AbuseIPDB is downloaded (in addition to the 3 free blacklists) and a threat status of each IP address is also obtained from the AbuseIPDB web site in real time. See AbuseIPDB Pricing for more details, a free service with limited checks is available (1000 queries / day as of November 2020).

Custom Block List: In order to incorporate third-party block lists, save the blocked IPs in the following format to the file %SYSTEMROOT%
Monitoring with EventSentry

\system32\eventsentry\temp\eventsentry_threatintel_custom.tmp. This file, when present, will be imported every time the other blacklists are downloaded:

IP;Confidence Score;Title

IP: IP Address
Confidence Score (optional): Number 0..100
Title (optional): Threat title or description

Example:
10.20.30.40;60;Port Scan
10.20.80.22;90;Web Attack,Port Scan,Spam

Optional fields can be omitted: “Confidence Score” defaults to 50 if not present, “Title” is set to “n/a” if not present. At minimum, one IP address per line must be specified.

The threat intelligence status can be used in event log filters and in the web reports to filter reports based on the threat status of an IP address.

Heartbeat Settings
Please see “Setting General Options” in the Heartbeat Monitoring chapter for more information on the general heartbeat settings.

5.3 Event Log Monitoring

An event log package is used to group one or more filters (usually more than one) into one logical entity that can then be assigned to one or more computers or groups. Filters are rules that define which events are being forwarded to which notification.

Event Log Package Options
In addition to the general package options, event log packages can be

- configured as “Catch-All Notification” packages
- configured to ignore exclude filters from other packages
- be triggered to be activated when a certain service is installed

See Package Options for more information.

Built-In Event Log Packages
NETIKUS.NET maintains a set of event log packages that contain common filter rules. These event log packages are installed automatically with EventSentry and can be updated automatically over the Internet. See Downloading Packages for more information.

Filters
Event log packages contain one or more filters and folders. For example, you can be emailed of certain errors from the Application event log, paged of certain events in the System log, yet forward all events (regardless of their properties) to a database. You can also apply thresholds to filters (for example to detect event log entries that occur at least X times during a given time period) and create recurring filters, which alert you when a certain event did not occur. See Filters for more information.

Applying Event Log Packages
To apply an event log package, right-click the package and select “Assign”. In the resulting dialog select a group or computer to apply the package to.
Creating and Deleting Event Log Packages

To create a new filter package right-click the Event Log Packages container and select Add Package or right-click a package and select Add.

To delete a package, right-click the package and select delete. All filters contained in the event log package will also be deleted.

5.3.1 Event Log Package Options

Event log packages offer additional options in addition to the general package options.

Catch-All Notification Package

It is recommended that you activate this feature on packages containing "catch-all" filters.

Catch-All Filters

We refer to a "Catch-All" filters whenever you have an include filter that will forward all events, for example all errors and warnings, to an action. Catch-All filter examples are:

- A filter forwarding all warnings, errors and audit failures to an email recipient
- A filter forwarding all audit success and audit failure events to a database

Since event logs generate a lot of noise, configurations with Catch-All filters usually also include many exclude and include threshold filters so that unnecessary alerts are not sent to the email recipient.

If you do not configure a package that contains a catch-all filter as a "Catch-All Notification Package" then include filters with thresholds from other packages might not work as expected.

Event Log Packages set to be Catch-All are processed after event log packages which are not set to be Catch-All packages. This makes sure that include filters with advanced features such as Thresholds are processed before filters in a Catch-All package.

Filter Chaining

Filter chaining is enabled on the package level and provides simple work-flow-like functionality. When enabled, EventSentry will generate an event (which can be linked to an action) when all filters in the package match in a configurable time period.

Ignore Exclude Filters from other packages

Exclude filters from all packages are, by default, always processed before a notification is sent out. That is, it doesn't matter in which package an exclude filter is contained - it will always apply.

If you have filters for which you would like to ensure that they are not excluded by exclude filters from other packages, then you can add them to a new package and configure the package to ignore exclude filters from other packages.

5.3.1.1 Filter Chaining

Filter chaining allows for an action to be triggered when two or more events occur within a configurable time period on the same host. All include filters which are part of the package will participate in the filter chaining. When all filters matched, the EventSentry agent will log event 10650 to the event log with relevant details.
Event log filters in a filter chaining package do not have actions associated with them; consequently a separate event log filter (in a different package) will have to be created in order to trigger an action.

Require Sequence
By default, filters can match events in any sequence in order to complete the filter chain. Enabling the "Require Sequence" option requires that events match the filters in the same order shown in the event log package.

When using a sequence, it's recommended to either not have any exclude filters in the package, or to position any exclude filters BELOW all of the include filters. Otherwise, the behavior of the filter chaining feature is undefined.

Timeout
The time period in which all filters of the event log package need to match an event.

Linking events through insertion strings
To ensure that events from unrelated activity do not complete the same filter chaining object, filters of a filter chaining package can be set to require one or more insertion strings to match. Similar functionality is also available for threshold filters.

Insertion strings are configured through the "Chain Settings" button which is displayed on the filter dialog in place of the "Advanced" button. When two or more filters have at least one insertion string configured, EventSentry will extract the run-time value of the insertion string(s) from the event and store them for the duration of the filter chaining time period.

Values of the extracted insertion strings need to match for all filters which have at least one insertion string configured. Not all filters in the package need to have an insertion string configured, those filters will always be considered a match as long as they satisfy the filter criteria.

5.3.2 Filters
Filters are an integral part of EventSentry and allow you create rules as to which event log record gets forwarded to which notification. The simplest EventSentry configuration for example would consist of a single filter forwarding all events from all event logs to a database.
Filter Processing

Since **Exclude** filters are always processed before include filters, it doesn't matter whether an exclude filter is located before or after an include filter, or located in a different package.

Include filters inside a package are still processed sequentially - from top to bottom. The sequence of include filters however is irrelevant in most scenarios, unless you use advanced features such as thresholds and "require acknowledgment".

The only exception are "Catch-All" packages and packages configured to ignore exclude filters from other packages, see **Package Options** for more information.

Filter Types

A filter can either be an **include** filter (and forward events to a notification) or be an **exclude** filter (and prevent events from being forwarded to a notification):

**Exclude Filters**

Exclude filters prevent certain events from being processed, and can either apply to all actions or only to a particular action. This gives you the ability to only exclude events for some actions (e.g. email), while logging everything to another action (event log consolidation). Exclude filters are **always** processed before include filters.

It does not matter into which event log package an exclude filter is placed, exclude filters are always evaluated before include filters are processed. The only exception are event log packages configured to **ignore exclude filters from other packages**.

Exclude filters are indicated in the filter list with a red "remove" button 🗑️.

**Include Filters**
Include filters process event records that match their filter criteria and pass them on to the configured action or all actions. The more fields you restrict in a filter (e.g. Source, Category, ID ...) the fewer events will match that filter.

You can also apply threshold settings to include filters, or configure include filters as summary notification filters.

Include filters are indicated in the filter list with a blue arrow 📈.

Recurring Event Filters
Recurring event filters appear like regular include filters, but do not actually forward events to a notification. Instead, recurring event filters write an *error* to the application event log when an event does *not appear* in the event log during a certain time period. For example, a recurring event filter can notify you when a backup job did not write a success event to the event log. See Recurring Event Filters for more information.

Filter Properties
You can filter events based on every property of an event record, including:

- Event Log (including custom event logs)
- Event Severity
- Event Source
- Event Category
- Event ID
- Event User
- Event Computer
- Event Description
- Day / Hour

See Filter Properties for more information. You can also paste event properties from an email sent by EventSentry or an event copied by the Windows event viewer into the general filter dialog.
5.3.2.1 Filter Properties

All fields in the Details section are not case sensitive and support wildcards, negation and multiple values separated by commas. Please see Advanced Text Processing for more information.

Pasting Event Properties

If you are creating a filter based on an event you copied to the clipboard from the Windows event viewer or have received via email from EventSentry, then you can automatically paste the key event properties (Event Log, Event Severity, Event Source, Category, Event ID and Username) into the dialog by clicking on any field and pressing CTRL+V.

Via Email: Open the email in your email client and select the event. If the email contains only one event then you should be able to simply press CTRL+A, otherwise select the event. If the email contains
multiple events and you select all of them, then only the first event will be used. When the event has been selected, copy it to the clipboard by pressing CTRL+C.

**Via Windows Event Viewer:** Open the event in question and click the **copy** button on the dialog.

Then, switch to the management console and either create a new filter or open an existing filter. Click on any field (e.g. Category) and click **CTRL+V**. All the key event properties with the exception of the event message should now have been filled in. Once the key event properties have been pasted you can customized the filter further by selecting between an include and/or exclude filter and so forth.

Please note that right-clicking and selecting "Paste" will not work with this feature, you have to click **CTRL+V**. As such, if you just want to paste text into one field in this dialog, right-click the field and select "Paste".

**Detailed Field Descriptions:**

**Name**
- The filter name is chosen by you and can be any text no longer than 128 characters. Filter names must be unique. The filter name may not contain a backslash (\).

**Actions**
- All actions that are to be notified (include filter) or not to be notified (exclude filter) when this filter matches.

**Trigger all actions**
- Check this checkbox to notify all configured actions instead of selected ones.

**Event Severity**
- Select which types of events this filter should match. "Audit Success" and "Audit Failure" are only relevant when you also monitor the **security event log**.

**Log**
- Select which event log(s) this filter should monitor. The event logs, "Directory Service" and "File Replication (Service)," are only useful on Windows 2000 (and higher) domain controllers. The event log "DNS Server" is only useful on Windows 2000 servers (and higher) when a DNS server is installed.

**Event Source**
- Specify which source this filter should match. If you do not specify an event source, the filter will match **any** source.

**Event Category**
- Specify which category this filter should match. If you do not specify an event category, the filter will match **any** category.

**Event ID**
- Specify which Event ID this filter should match. You can separate multiple Event IDs with a comma, for example “3,5,118”. Event ranges (e.g. 4000-500) and negation (e.g. !4624) are also supported.

Event IDs are **only unique within an event source**. As such, always specify an event source when specifying an event id. Otherwise, a filter may match other events it was never intended to match.

**Username**
- Specify which username this filter should match. This is currently only relevant for the **security event log**. Usernames are logged by the Operating System in the form **DOMAIN\Username**.
Computer
Specify which computer this filter should match. If you do not specify a computer name, the filter will match any computer the package is applied to.

When FQDN names are enabled, specify the fully qualified host name (e.g. mailserver.mydomain.com), otherwise specify the NetBIOS name.

Filter Type
- Include: The matching event will be forwarded to the specified action(s)
- Exclude: The matching event will be blocked from being forwarded to the specified Action(s) (or no actions if "Trigger all actions" is checked)

Advanced
Clicking Advanced will bring up the advanced options dialog.

Content Filter
Utilize the Content Filter to filter against a certain text string instead of or in addition to the properties listed above. Click the + button to add a new condition to the list list of content filters, or select a string and click the - button to remove it from the list.

If you specify multiple content filters, then you can chain them either with a logical OR or a logical AND. Content filters are processed from the top down.

OR: The content filter matches as soon as the first condition matches.
AND: The content filter only matches when all listed conditions match.

Using multiple negation filters in combination with an OR condition is not recommended as it may lead to unexpected results.

Notes
You can annotate filters with personal descriptions which might provide useful to co-workers or yourself in the future.

Day and Time Restrictions
Please see the Day & Hour page for details.

5.3.2.1.1 Content Filter
The content filter field allows you to filter and process events based on their event message text. Content filtering distinguishes between the following:

- Wildcard match of the entire event message (default)
- Insertion string match
- Regex match (Perl syntax)

Wildcard Match
With this option, the specified text will be matched against the entire event message text (aka event description). You can either use wildcards in your content filter, or specify a 1:1 match.

Insertion String Match
Most events that are logged to the event log and contain dynamic information contain one or more insertion strings (click here for a detailed discussion on event message files and insertion strings). While
a basic wildcard match is sufficient in most cases, the insertion string match gives you the following benefits:

1. No complex queries have to be crafted in order to match a subset of the event message
2. Additional comparison types (e.g. numerical) are available for insertion strings

With the insertion string match, you can not only perform textual comparisons of insertion strings, but also the following:

1. Numerical comparison (less than, equal, not equal, more than)
2. File checksum comparison
3. Group membership check

Using insertion string variables (e.g. $STR2) in the Content Filter field is supported and allows for insertion strings to be compared with each other at run time.

1. Numerical comparisons
   When you select one of the numerical comparisons for an insertion strings, then EventSentry will convert the textual insertion string to a number, and then perform the select numerical comparison on that string. Numerical comparison supports floating point numbers.

   **Note:** Only use this option if the insertion string is a number.

2. File checksum comparisons
   Treats an insertion string as a filename, and creates a SHA-256 checksum of the file. The checksum you specify is then compared with the checksum of the file.

   **Important:** Only use this options 2 and 3 if the insertion string points to a file name. Do not use this option with events that occur at a high frequency or with insertion strings that point to large files, as checksum generation may use a significant amount of CPU time.

3. File entropy comparisons
   Similar to the checksum comparison, treats an insertion string as a filename and calculates the entropy (randomness) of a file. The entropy is returned as float number with a range from 0 to 10. The more random a file, the higher its entropy. This can be used to detect a Ransomware outbreak which creates a large number of files with a high entropy. In practice, compressed and encrypted files have a high entropy.
You can check the entropy of a file with the `/e` option of the “checksum.exe” utility of the EventSentry SysAdmin Tools.

4. Group membership check
Treats the insertion string as a username, and verifies whether the username is a member of the group you specify. To avoid ambiguity, it is recommended that specify group names with the domain or host name, for example `DOMAIN\GroupA` or `SERVERB\GroupX`.

Only use this option if the insertion string points to a valid username. Do not use this option with events that occur at a high frequency, as group verification may be time consuming (relatively speaking) and use large amounts of CPU time.

5. Malicious IP Address Check
Checks whether an IP address from an event log event is listed in any of the downloaded blacklists (also checks AbuseIPDB if configured). The filter will only match if the IP address is deemed malicious. Only works for collector-enabled actions, since the IP address check is performed on the collector. Requires that Threat Intel is enabled.

6. Wildcard comparison (“matches”)
Similar to the wildcard match, but this option matches the selected insertion string against the specified text.

7. Command line arguments
Counts the number of command line arguments contained in a string, taking quotes etc. into consideration, allowing to filter if the number of arguments are fewer than, equal to or exceed a certain count. This can be useful for detecting certain malware or other anomalies.

If both an event source and event id are specified in the filter properties and the message file is correctly registered, then the Preview button can be used to see the event template and its insertion strings. The event message browser can also show the available insertion strings of an event.

The table below shows the types of strings expected by the individual comparisons:

<table>
<thead>
<tr>
<th>Match Category</th>
<th>Expected type of string in &quot;Content Filter&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>matches</td>
<td>any string</td>
</tr>
<tr>
<td>matches file checksum</td>
<td>Filename with complete path</td>
</tr>
<tr>
<td>is member of group</td>
<td>Username</td>
</tr>
<tr>
<td>numerical</td>
<td>any number</td>
</tr>
</tbody>
</table>

Regex Match (Perl Syntax)
Supports case insensitive text matching based on regular expressions. EventSentry uses the PCRE engine, please see Regular Expressions for the complete syntax.

The most common regular expression metacharacters are:

- `^` matches the beginning of the event message text
- `$` matches the end of the event message text
- `.` matches any characters
- `\s` matches a whitespace character
- `\d` (\D) matches a decimal digit (non-digit)
- `\` quote the next metacharacter
- `[]` sequence, e.g. `[a-z]` matches all lowercase letters from a-z
Since an event message text will often consist of more than one line, the `^` symbol will always match the beginning of the event message, even if the event contains multiple lines. Equally, the `$` symbol will always match the end of the entire event message text, and not the end of the first line.

In addition, regular expressions support the following quantifiers:

- `*` match 0 or more times
- `+` match one or more times
- `?` match 1 or 0 times
- `{n}` match n times
- `{n,}` match at least n times, but no more than m times
- `{n,m}` match at least n times, but no more than m times

The table below shows basic regular expression examples:

<table>
<thead>
<tr>
<th>Text</th>
<th>Matching regular expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opera 11.61 (Opera Software ASA) was installed.</td>
<td><code>^Opera\s\d+.\d+.\d+.installed.$</code></td>
</tr>
<tr>
<td>Computer TEST3-WIN2K8 booted.</td>
<td><code>^.*TEST\d-WIN\dK\d.\d.\d.\d.*$</code></td>
</tr>
<tr>
<td>User RENAULT\francois3 logged on.</td>
<td><code>^User\s\[A-Za-z]+\[A-Za-z0-9]+ \log</code>ed on.$`</td>
</tr>
</tbody>
</table>

**Negation**

You can use the negation character (exclamation mark, `!`) for any text-based matching. Please see [Advanced Text Processing](#) for more information.

### 5.3.2.1.2 Advanced

#### Stop Processing

Checking this box will prevent any filters below this filter in the same package or filters in packages below the current package from being processed.

#### Require Acknowledgment

When consolidating events to a database, one can require select events to require a manual acknowledgment. This is usually useful for critical events that need to be reviewed and manually "cleared" or "acknowledged".

For example, you can create a filter for events that pertain to a failed backup event. If a backup fails, then this event will show up in the web reports as "pending acknowledgment", requiring an administrator to document what action was taken to resolve the issue.

If one filter matching the event has "Require Acknowledgment" set, then the acknowledgment flag will stick, even if other matching filters do not have this setting enabled.

#### Email / Network Action Overrides

By default, all events are forwarded as-is, which can be overwhelming for some users. The "Override" feature allows the user to define the subject/title as well as content of an email or network message. The subject/title or message can either be a static text or may contain any variables from the event itself (e.g. insertion strings or event properties). The screenshot above shows two insertion strings from a 4625 security event being used.
If an email contains more than one event then the email message body will not be overwritten and instead revert back to the "default" where the content of every event is listed.

**Insertion String Override**

Even though most events utilize message DLLs supporting the ability to create filter rules based on insertion strings, some events either do not use message templates or include long dynamic content where insertion strings do not help.

For example, when EventSentry logs the content of a log file or an incoming Syslog message, that content is simply injected into the respective EventSentry event. If the (log file) content follows a known pattern, EventSentry can redefine the insertion strings of the event based on a regular expression pattern. The original insertion strings are always lost since they are replaced.

<table>
<thead>
<tr>
<th>Event</th>
<th>Template</th>
<th>Actual Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Text matching one or more filter rules has been found in file %1: %2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2016-10-22 07:20:04 12.31.29.171 GET /index.php - 443 - 12.31.29.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mozilla/5.0+[en]+(X11,+U;+OpenVAS+8.0.7) 404 0 2 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR1 = C:\INETPUB\LOGS\LOGFILES\W3SVC1\u_ex161022.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR2 = 2016-10-22 07:20:04</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.31.29.171 GET /index.php - 443 - 12.31.29.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mozilla/5.0+[en]+(X11,+U;+OpenVAS+8.0.7) 404 0 2 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR2 = 2016-10-22 07:20:04</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.31.29.171 GET /index.php - 443 - 12.31.29.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mozilla/5.0+[en]+(X11,+U;+OpenVAS+8.0.7) 404 0 2 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR3 = 12.31.29.171</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR4 = GET</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR5 = /index.php</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR6 = -</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR7 = 443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR8 = -</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR9 = 12.31.29.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR10 = Mozilla/5.0+[en]+(X11,+U;+OpenVAS+8.0.7) 404 0 2 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR11 = 404</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR12 = 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR13 = 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$STR14 = 0</td>
</tr>
</tbody>
</table>
5.3.2.2  Advanced Text Processing

**Comma Separated Values (Event Log Filters only)**
You can separate multiple values with a comma to avoid creating multiple filters. Simply combine all the values the field should match with commas and **make sure you are not using a space after or before the comma**. For example:

```
Print, MrxSmb
```

Supported by all fields in the “Details” section.

**Negation Symbol (Event Log Filters only)**
You can negate a value by pre-pending it with an exclamation mark. For example, to match all events except for those with the source of Print you could use the following:

```
!Print
```

or

```
!*Print*
```
Wildcards
The wildcards * and ? are supported.

*  matches zero or more occurrences of any character
?
matches one occurrence of any character

Note: Filter strings, whether containing wild cards or not, are never case sensitive.

Examples

<table>
<thead>
<tr>
<th>Filter with wildcard</th>
<th>Matches string</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipx*</td>
<td>IPXCP</td>
</tr>
<tr>
<td></td>
<td>IPXRIP</td>
</tr>
<tr>
<td></td>
<td>IPXRouterManager</td>
</tr>
<tr>
<td></td>
<td>IPXSAP</td>
</tr>
</tbody>
</table>
| *iptables*proto=*   | syslog@netikus-router[kern.debug]: kernel: IPTABLES INPUT: IN=ppp0 OUT= MAC=
| ?p*dpt=13*          | SRC=65.35.223.155 DST=65.41.63.146 LEN=48 TOS=0x00 PREC=0x00 TTL=114
|                      | ID=54221 DF PROTO=TCP SPT=1429 DPT=135 WINDOW=64240 RES=0x00 SYN
|                      | URGP=0         |
| VMnet*               | VMnetAdapter   |
|                      | VMnetBridge    |
|                      | VMnetDHCP      |
|                      | VMnetuserif    |
| *rip*                | IPRIP2         |
|                      | IPXRIP         |

5.3.2.3 Filter Processing

The following rules are important when setting up filters in multiple packages.

1. Only filters from global or assigned packages will be processed.

2. A notification is never processed more than once. If two filters configured for the same notification match an event, that event will still only be forwarded to that notification once.

3. Exclude filters from all packages are always checked before an event is forwarded to a notification. Exception: An event log package is configured to ignore foreign excludes - in this case only exclude filters from the same package as the include filter are checked.

4. Filters from Catch-All packages are always processed after filters from Non-Catch-All packages.

5. If an include filter with a threshold setting matches an event, then any subsequently matching filter will not process the event.

6. Packages are processed in the order show in the management application with the exception of Catch-All packages which are always processed after regular packages.
Please see the flowchart below to see how filters are processed:
5.3.3 Folders

You can use folders to group related filters into folders, which is useful for organizing large amount of filters. Currently, one level of folders is supported (you cannot create subfolders of folders).

Creating Folders
You can create a folder by right-clicking a filter or event log package and selecting "Add Folder":

Properties
- Assignment -
  Global
  Assign ...
- Event Log Filters -
  Add Filter
  Add Filter using Wizard
  Add Folder
  Sort Filters
  Paste
- Packages -
  Add Package
  Rename
  Disable
  Hide
  Delete
Help
Once the folder has been created, you can either create new filters in the folder by right-clicking the folder and selecting **Add Filter** or by moving/copying existing filters into the folder. A common scenario for folders is to group exclude filters into one folder.

**Deleting Folders**
If you delete a folder then all filters within that folder will also be deleted.

**Moving Filters into Folders**
You can move existing filters into a folder in two ways:

1. Move the filter onto the folder. The filter will be positioned immediately after the folder, as the first filter within the folder.
2. Move the filter onto a filter in the folder. The filter will be positioned after the filter it was dragged on to

**Creating Filters in Folders**
Right-Click the folder and select **Add Filter**. The filter will be created in the folder.

**Removing Filters from Folders**
To remove a filter from a folder you can either move the filter outside the folder (for example by moving it onto another filter) or by right-clicking the filter and selecting **Remove from Folder**. The filter will then be moved outside of the folder at the end of the filter list.

5.3.4 **Editing Filters**

**Adding Filters**

- right-click the event log package where you would like to add the new filter and select **Add Filter**
- right-click an existing filter and select **Add**

You will then be able to type a name for the new filter and press **Enter**. Continue by configuring advanced filter options.

**Editing Filters**

- left-click (or double-click, see usability) the filter item in the left pane
right-click the filter object and select **Edit**

The filter details will then be loaded into the right pane and the active filter object in the left pane will become bold.

**Deleting Filters**

- right-click the filter and select **delete** from the menu
- select the filter object and press the **Del** button on the keyboard

The filter will then be deleted.

**Renaming Filters**

- right-click the filter and select **rename** from the menu
- select the filter and press the **F2** button on the keyboard (only works with usability set to double-click)
- left-click the filter object for 1-2 seconds

You will then be able to type a new name for the filter.

**Cut, copy, & paste**

1. Click the filter object in the left pane and make sure that it is selected
2. Click the **cut** or **copy** symbol in the toolbar or choose **Cut / Copy** from the **Edit** menu
3. Select the position where you would you like to insert the filter object. This can be
   - a **group** if you would like to move the filter object into a new group
   - a **filter** in the **same group** if you would like to re-order the filter object
   - a **filter** in a **different group** if you would like to insert the filter object into a different group
4. Click the **paste** symbol in the toolbar or choose **Paste** from the **Edit** menu

If a filter object with the same name already exists then #1, #2 ... etc will be automatically appended to the name.

**Moving filters up / down**

To quickly change the order of a filter you can move a filter up or down respectively. To move a filter up or down simply right-click the filter and choose either **Move Up** or **Move Down**.

**Dragging & Dropping filters**

You can drag & drop filters to copy or move them.

- To move a filter simply left-click the filter object and drag it to a different position or a different group
- To copy a filter simply right-click the filter object and drag it to a different group (to copy filter objects in the same group please use the copy/paste feature).

**5.3.5 Thresholds**

Filter thresholds enable you to not only take action when a certain event occurs, but also depending on **how often** the event occurs. Some threshold scenarios:

- Be notified if an event occurs X number of times within a specific time period
- Prevent events from flooding an action
- Detect lateral movements throughout a network (requires collector)
• Detect if users log on with a wrong password more than X times

Thresholds are setup on a per-filter basis, and you can access the threshold settings by editing a filter and clicking on the **Threshold** tab. Set a threshold to either “Agent-Side” or “Collector-Side” to activate threshold settings for a filter. Filters with thresholds are shown with a little ruler 📏 in the list.

**Threshold Type**

**Agent-Side**
These thresholds are executed on the agent, the only type of threshold supported until v3.3. Agent-side thresholds should always be preferred unless correlation of events occurring on multiple hosts is necessary. Required for filters that are part of a [filter-chaining package](#).

**Collector-Side**
These thresholds are executed on the collector, and require that:

• a collector is installed and running
• the referenced action of the filter uses a collector
• no agent-side thresholds are processed before the collector-side threshold
• the filter is not part of a [filter chaining package](#)

Collector-side thresholds make it possible to correlate and evaluate events from multiple hosts in order to detect threats and patterns that involve more than one host. For example, lateral movements can be detected by analyzing certain logon events.

The “Computer” event and the “Group By” options are only available for collector-side thresholds.

---

**When the primary purpose of a collector-side threshold is to detect activity rather than suppress (e.g. all check boxes under “Event Processing” are unchecked), then it's recommended to associate an action that already processes the events in question (e.g. a database action) when possible - rather than assigning a different action (e.g. email).**

For events that occur often this can reduce the data volume by ensuring that events are not transmitted twice - once for each action.
Threshold Interval
Specify the threshold interval, for example 20 events in one hour.

Event Processing
Allows you to configure whether events are forwarded to the configured notification before and/or after the threshold has been met. You can either check all, one or none in this section.

Forward events until threshold is reached
Checking this box means that events matching your filter will be processed (and forwarded to the notification) until the threshold is met.

Forward events after threshold has been met
Checking this box means that events matching your filter will be processed after the threshold has been met.

Forward first event only
You can configure a threshold filter to only forward the first event after a threshold has been met, instead of forwarding all events after the threshold has been met.
This is particularly useful when working with events from the security log. When you configure a threshold for a failed-login type of filter (e.g. notify me when there are more than 5 failed logins in 5 minutes), then you will usually not want to receive the first failed login attempts, since users type in wrong passwords all the time. If the threshold is exceeded however, you probably do want to know which user is trying to log in. If you just configure the filter to forward all events after the threshold, then you will get an email for every wrong password attempted, which is usually also not desired. Instead, you configure the filter to only forward you the first event after the threshold has been exceeded, and then write an event to the event log when the period has expired to indicate how many failed logon attempts there have been for this user account.

Selecting none of the two check boxes is allowed when you check at least one check box in the "Event Logging" section. In this case the filter will never forward any events, but write an event to the event log when the threshold has been met.

**Event Logging**

This section controls whether events will be generated and logged to the application event log when the threshold is met, and/or when the threshold period is complete.

- **Log when threshold is met**
  Checking this box results in an event being written to the Application event log immediately when the filter meets its threshold.

- **Log when threshold is met/exceeded and interval is elapsed**
  This option is similar to the first one, except that this feature will log an event only after the threshold has been met and the threshold interval has elapsed. The advantage of this option is that the event logged by the threshold filter will let you know how many events have been processed by this filter, and how many were dropped.

- **Log as**
  Specify whether you would like events logged as Error, Warning or Information events. Please see Event Logs for more information as to which events are logged to the event log by this feature.

**Threshold Matching**

By default the internal counters (that count towards the threshold limits) are increased every time an event matches a filter (Filter setting). While this is desirable in most cases, you can also have threshold counters be applied to event records, which allows for more granular threshold settings but is slightly more resource consuming.

- **Filter (every event processed by this filter)**
  Every time an event matches the filter the internal threshold counters are increased. This is the recommended option for threshold filters applied to events that are not from the Security event log.

- **Event Properties / Insertion Strings (every event sharing properties)**
  Every event that has the same values for the selected properties will increase the internal threshold counters, this feature is mostly useful for events from the Security event log, for example to analyze failed logins. Instead of every event counting towards the threshold, only events that share certain event properties, including insertion strings if selected, will count towards the total counter.

The "Computer" field is only available for Collector-Side thresholds, since the "Computer" property is always the same for Agent-Side thresholds.

The diagram below illustrates how matching based on event properties and insertion strings works. In this example, a filter processes 4624 events and uses insertion string 5, which represents the "Security ID", as the unique identifier. Consequently, virtual threshold objects for each unique occurrence of an encountered Security ID are created. When the same Security ID is encountered 4 times within 3 minutes, an alert will be immediately generated - UserC in this example. Another alert will be generated when the threshold period, 3 minutes, is elapsed.
**Group By (Collector-Side)**

By default, thresholds are increased whenever an event matches a filter or the selected event properties. Using the "Group By" feature will compare the number of groups created against the threshold instead of the number of events.

The diagram below illustrates how matching based on event properties and insertion strings in combination with grouping by computer works to detect lateral network movement. In this example, a filter processes 4624 events and uses insertion string 5, which represents the "Security ID", as the unique identifier. Instead of just counting the occurrences of Security IDs however (as shown in the previous example), the threshold object keeps track of all the different computer names encountered instead.
In the example below, UserA logged on to 5 different hosts, resulting in the threshold limit of 4 being exceeded. While the total number of logons for that user is being recorded (8), that number does not count towards the threshold. Only the unique number of computer values (5) is evaluated. UserB on the other hand only logged on to one unique computer, a total of 3 times.

### Event Logs

Currently the following event log records can be logged by this feature:

<table>
<thead>
<tr>
<th>Type</th>
<th>Event ID</th>
<th>Source</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Event log filter Logon Failures exceeded the configured threshold (20 entries / 3600 second(s)). 5 events (out of a total of 25) were dropped by this filter. You can review the dropped events in the event log or the web reports. The matching events and their frequency were:

[ID=4771][LOG=Security]:10
[ID=4624][LOG=Security]:10

Event log filter Sample Threshold Filter has reached the configured threshold (20 entries / 600 second(s)). The matching events and their frequency were:

[ID=10100][LOG=Application]:20

Event log filter Sample Filter has reached the configured threshold (100 entries / 1200 second(s)). Events matching this filter will now be processed. The matching events and their frequency were:

[ID=4688][LOG=Security]:100

Event log filter Sample Filter has reached or exceeded the configured threshold (10 entries / 600 second(s)). 12 events were processed during the interval. The matching events and their frequency were:

[ID=4771][LOG=Security]:6
[ID=4624][LOG=Security]:6

The limit of a threshold object has been reached, events will continue to be forwarded to the associated action:

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Event Details:
%7
The limit of a threshold object has been reached, events will continue to be forwarded to the associated action:

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Events Summary:
%8

Event Details:
%9
The limit of a threshold object has been reached, the next matching event will be forwarded to the associated action:

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Collect or-Side 1203 EventSentry Collector

A threshold has been met (with group field)

Events forwarded: %5
Description: %6

Event Details:
%7
The limit of a threshold object has been reached, the next matching event will be forwarded to the associated action:

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Events Summary:
%8

Event Details:
%9
The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires:

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Collect or-Side 1205 EventSentry Collector

A threshold has been met (with group field)

Events Summary:
%8

Event Details:
%9
The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires:

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Collect or-Side 1206 EventSentry Collector

A threshold has been met

Events forwarded: %5
Description: %6

Event Details:
%7
The limit of a threshold object has been reached, events will be forwarded to the associated action until the threshold expires and event ID 1220 is logged.

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Event Details:
%7
The limit of a threshold object has been reached, events will be forwarded to the associated action until the threshold expires and event ID 1220 is logged.

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Events Summary:
%8

Event Details:
%9
The limit of a threshold object has been reached, the next matching event will be forwarded to the associated action until the threshold expires and event ID 1220 is logged.

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Event Details:
%7
The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires and event ID 1220 is logged.

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Event Details:
%9
The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires and event ID 1220 is logged.

Name: %1
Identifier: %2
Limit: %3 event(s)
Time remaining: %4 seconds
Events forwarded: %5
Description: %6

Event Details:
%7
The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires and event ID 1220 is logged.
5.3.6 Timers

Filter timers give you the ability to ignore an event - even if it matches one of your filters - if a particular subsequent event occurs within a configurable amount of time.

Consider the following scenario: A critical service stops but is automatically restarted within 1 minute (e.g. after an AntiVirus engine has updated itself), resulting in two events generating an event in the event log. First, when the service stops and again when the service is restarted. You could of course stop the service from being monitored altogether, but that would not be desirable since you would want to be notified when the service stop without being restarted. Filter-Timers offer a solution to this problem.

Filter timers solve this problem by letting you create two filters: One filter to match the first event, and one to match the subsequent event which, in turn, clears the first alert. As such, you will never be notified of the original event if it has been cleared within the timeout period.

Keep in mind, that due to the nature of this feature you will not be notified of an event matching a filter with the Enable Timer option set, until the timer period has elapsed.

Enabling a Timer

To enable a timer on filter, edit the filter and click on the Timers tab. On the Timers tab, select “Enable Timer” to activate the timer. Then, specify a timeout period (e.g. 2 minutes) and specify a filter that will clear the timer by clicking the plus + button. Clicking this button will bring up a dialog showing all suitable filters (e.g. include filters) that can be used to clear this timer.
The "Clearing" Filter

This filter is referenced by a timer filter, and has the ability to clear the timer. When setting up this filter, specify the same action as the action specified in the timer filter. If this filter matches while a timer filter is counting down from the set timeout, it will clear the timer, and the action will not be notified.

If the clearing filter matches an event while no timer is active, it will behave like a regular filter. As such, you can specify multiple actions on the clearing filter.

Insertion Strings

This feature is particularly useful when creating a filter timer that should match a variety of events. For example, a "service stop / service start" combination, a "process end / process start" combination or a "logon / logoff" combination. Without utilizing the insertion string feature, it would be necessary to create a filter pair for every unique event (e.g. service).

Let's say that you want to be notified if any monitored service were stopped for more than 5 minutes (or if a host is offline for more than 5 minutes etc). Let's assume that the DNS Server service were stopped, which would trigger a timer that would expire in 5 minutes. Let's also assume that the License Logging service were started on the same host 3 minutes after the DNS Server service was stopped. Because they both matched the generic filter that catches service start events, the timer would be cleared and you would not be notified of the stopped service.

Using insertion strings however, you can force EventSentry to compare the selected insertion strings from the originating event that set the filter timer, and the timer that is about to clear the filter. If they match, then the filter timer is cleared, otherwise it is not. We recommend that you use the Event Message Browser to determine the number and position of insertion strings inside events.

Consider the following EventSentry events that pertain to service monitoring as well as process creation / termination

<table>
<thead>
<tr>
<th>Event Source</th>
<th>Event Category</th>
<th>Event ID</th>
<th>Event Description (insertion strings start with % character)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventSentry</td>
<td>Service</td>
<td>10100</td>
<td>The status for service %1 (%2) changed from %3 to %4.</td>
</tr>
</tbody>
</table>
Whenever EventSentry records a service status change, it logs event 10100 to event log, and substitutes %1 with the name of the service whose status changed. As such, if require a match of insertion string #1, then an event pertaining to the “License Logging” service cannot clear the timer that was set from the “DNS Server service”.

A similar setup could be achieved with the events logged by Windows when a user logs on and then logs off again. If we set a filter timer based on event 4624, and the filter clearing timer based on event 4647, then we need to connect insertion string #8 of the logon event with insertion string #4 of the logoff event.

When specifying insertion strings, both the insertion from the filter timer event AND the clearing event need to be specified. The same insertion string may be specified for both events if they are the same (in the examples above the insertion strings are the same for the service monitoring event but not for the logon/logoff events).

How it works
When an event matches a timer-enabled filter, EventSentry will wait until the timeout period has elapsed before it will forward the event to the configured notifications. EventSentry will append the string TIMER-DELAY to the subject of an email if one of the configured notifications is of type SMTP.

If the filter specified in the “Filter that can clear this timer” list matches an event within the timeout period, then the neither the original nor the “clearing” filter will process the notification, the objective of this feature.

Controlling Notifications
The point of a filter timer is of course to suppress notifications if the event starting a filter timer is cleared within the configured time period. Consequently, there is no scenario where EventSentry would send out a notification if the timer filter is cleared.
It is possible to control whether notifications are sent out if the event clearing a filter timer happens outside the configured time window. For example, a filter timer for a service is configured for 3 minutes, but the service is restarted after 4 minutes. Depending on the circumstances, it may or may not be desirable to receive a notification when the filter clearing the timer processes the event.

**Receiving a notification**
To trigger a notification when the event happens outside the configured time window, simply configure the same action on the clearing filter as on the timer filter. If the event that is supposed to clear the timer happens delayed, outside the timer window, then it will trigger a notification. In the case of the service monitoring example, this would inform the user that the service was ultimately restarted, albeit with a delay.

**Suppressing notifications**
To suppress notifications and strictly get notified that the filter timer expired, then no action should be specified on the timer clearing filter. This will still clear the timer filter if the event happens in the specified time window, but will not send any notifications if the event occurs outside (after) the time window.

---

5.3.7 **Advanced Hour / Day Settings**
The Hour / Day settings allow you to restrict your filters further or perform additional tasks.

**Filter Day & Hour Configuration**
The Filter day & hour configuration allows you to set a filter active/inactive for certain hours of the week (more information).

**Filter Expiration**
Filters can be configured to automatically expire at a certain date/time in the future (more information).

**Boot Behavior**
Filters can be configured to only be active during or after the system has finished booting (more information).

**Summary Notification**
Summary notifications allow you to receive a summary email at certain times during the week/day, instead of receiving emails immediately. This feature can also be used in connection with an ODBC notification (more information).

**Recurring Events**
You can become notified if a certain event **does not** appear in the event log during a certain time period, for example an event confirming that a backup job was successful (more information).

### 5.3.7.1 Day & Hour Configuration

In addition to the General Filter Options you can also define the day or time a filter is active. If, for example, you are not interested in receiving event records from the security event log during the day, then you can disable the filter during certain hours of the day.

To change when a filter is active, set the “Schedule Type” to “Normal”, add one or more schedule and specify whether the filter will be **active** or **inactive** during the schedules listed below. Other available schedule types are “Summary” and “Recurring”.

Filters with a schedule are shown with a small clock ☐ in the tree.
Filter shown above will only be inactive during the week from 8AM to 6PM.

Applying a filter to the "nth" day of the month

By default, the above hour/day schedule is active every week of the month. The schedule can be restricted to only apply on every nth week of the month by changing the "Apply To" setting. For example, the schedule below would restrict a filter to only be active every 2nd Tuesday of the month. This could be useful for an exclusion filter which excludes certain events during a monthly patch schedule for example.

A full day schedule is indicated with 00:00 to 00:00
5.3.7.2 Expiration

You can configure to expire a filter by checking the "Filter Expires" check box on the Hour / Day tab. This enables you to create rules that will stop working at a particular day you set.

For example, you might be getting recurring email alerts for a particular problem that you are aware off. This problem is being addressed, but it will take three days to resolve it. As such, since you are aware of the problem you would probably prefer not to get alerts until the problem is supposed to be resolved.

If you simply create an exclude filter for the alert, then you could potentially forget about the problem. Instead, you can still create an exclude filter but this time set the exclude filter to expire at a particular day. In the example above, you would set the filter to expire right after the problem is supposed to be resolved. This way, you will continue to receive email alerts if the issue has not been resolved in time.

5.3.7.3 Boot Behavior

Filter rules can be configured to only be active after a system has finished booting (when the uptime > 5 minutes), which can reduce unnecessary alerts that are only generated during the boot process. The boot behavior option supports three different settings:

1. Always Active
The filter is always active, regardless of whether the system is booting or not. This is the default.

2. Only During Boot
The filter is only active during system boot.

3. Only After Boot
The filter is only active after the system has finished booting.

A filter that is only active during the boot process can be useful to exclude certain alerts that are only generated during the boot process. A filter that is only active after the boot process has completed will not alert on potential noise that is generated during the boot process.
5.3.7.4 Summary Notifications

Summary notifications collect and cache events instead of forwarding them to an action immediately. When the schedule ends, all cached events are forwarded to the intended action in one batch. Filters with a summary schedule are shown with a little clock in the list. Jobs in the web reports are generally recommended over summary notifications since they can summarize events from multiple hosts and support multiple output formats.

Summary filters can work with any action except for the special setting "Trigger all actions". Summary notifications are bound to a particular action. It is not recommended to create multiple summary notifications which use the same action; instead, a new action should be created for each summary notification.

When configuring a summary schedule, the listed schedule specifies the time period when events are being collected and cached. Events are forwarded to the notification listed on the "General" tab when the schedule ends (e.g. 5PM in screenshot listed below).

The filter will not match any event outside the listed schedule(s).
Collects events Mon-Fri that occur between 8am and 5pm, and sends out a summary email Mon-Fri at 5pm

**How it works**

If an event occurs during a list schedule, then the event will be collected. The collected events are sent out when the schedule ends.

**Example above:** Events which occur between 8am and 5pm from Mon through Fri will be collected and cached. Every weekday at 5pm, the collected events will be forwarded to the configured action. Events occurring on weekends or outside the 8am-5pm schedule will not match this filter and thus not be processed.

**Real World Scenarios**

One can use the summary notification feature in a number of scenarios:

- Receive one summary email every Monday morning
- Send a weekly summary email to a supervisor containing all error events of the week
- Log events to a database only twice a day to save bandwidth from a server connected through a slow link
Service Restarts
Summary events are retained when the EventSentry service restarts. Collected events are written to a temporary file in the EventSentry temp sub directory and start with "eventsentry_summary_" and are processed when the service starts.

See the section Summary Notification Examples for examples.

5.3.7.5 Recurring Event Filters

If events are expected to occur on a regular basis (e.g. a backup event), then a recurring event filter can notify the user when the event did not occur. To activate this feature set the Schedule Type to Recurring Event. Recurring filters are indicated with a circle arrow in the list.

Activating this feature will disable the “Actions” area in the "General" tab. Unlike regular filters, a recurring event filter does not notify a action, but instead only writes an error event to the application log (see "Event Log" below) when the required event(s) did not appear during the specified time period. As such it is imperative that another filter is in place that will notify the user of this error event, for example by email.

Setting the Time Periods
After setting the general filter properties on the “General” tab, add one or more schedules to the list when the event is supposed to occur. A schedule can either be a time frame (e.g. Mon, Tue from 2am to 5am) or an interval (e.g. every 10 minutes).

If the event does not occur during the time frame or interval, EventSentry will write an event to the event log indicating that the filter did not match any events.

In the example below, an event needs to appear between 12:00 AM and 7:00 AM every day, Tuesday through Saturday. On Sunday the event needs to appear between 5:00 AM and 12:00 PM.

Intervals
Instead of a fixed time frame, a recurring filter can be configured to require the filter to be matched every X minutes or hours. When setting an interval, the weekday and "From / To" settings still apply. This allows for a flexible configuration where you can require an interval only during certain hours of the day.
5.3.8 Monitoring Custom Event Logs

With Custom Event Logs you can categorize event records by their event source and store them in a separate event log. This can be useful if you would like to organize events by their source. In so doing, you are redirecting the log entries to an event log that you specify.

For example, you can create a custom event log called Web Server, which stores events from the sources IISADMIN, SMTPSVC and VBRuntime.

Events from these specified sources are written to a different event file (and not written to the default event log file). Custom event log files are stored in the %SYSTEMROOT%\SYSTEM32\CONFIG directory by default; the same location where the default log files (Application, Security, System etc.) are stored.

EventSentry makes it easy for you to manage custom event logs without requiring you to manipulate the registry manually. EventSentry takes care of creating all registry keys and registry values. It even takes
care of moving message file information into the custom event log so that viewing event details works as expected.

You can also monitor these custom event logs with EventSentry, which will support a maximum of 30 custom event logs (in addition to the 3-6 default event logs).

EventSentry does not support monitoring the “Forwarded Events” or “EventCollector” event logs. All other event logs can be monitored in real time.

5.3.8.1 Managing Custom Event Logs

Custom event logs can be managed with the Manage Custom Event Logs dialog. To open this dialog click on

- Manage Custom Event Logs in the Tools menu

or click on

- Manage Custom Log Files in the Custom Event Logs tab of any filters’ details.

The dialog shows all custom event logs and, after clicking on a custom event log, their associated event sources:
Creating a Custom Event Log
Type the name of the custom event log into the Custom Event Log Name field and click the Add button. A custom log file will automatically be created in %SYSTEMROOT%\SYSTEM32\CONFIG by the Operating System. After the custom event log is created you can assign event sources to this log.

Deleting a Custom Event Log
To delete a custom event log select the log from the All configured custom event logs list and click the delete button. The log file itself can be moved or deleted manually from %SYSTEMROOT%\SYSTEM32\CONFIG directory after a reboot.

Deleting a custom event log will remove all associated event sources. To avoid losing message file information, remove all associated event sources manually from the affected log (see below) before removing the custom log itself.

Associating an Event Source with a Custom Event Log
Custom event logs will only work if you associate event sources with them. The associated event sources will then be written to the custom log file rather than to one of the default log files.

You can either associate

1. new event sources with the custom log (e.g. if you are developing a (web) application that will log to the event log)
2. assign existing event sources from another event log (e.g. Application)

1. New Event Sources
If you intend to create new event sources then only the registry key

HKLM\System\Current Control Set\Services\Event Log\Your CustomLog\Your NewSource

will be created. You will have to manually register a message file DLL if you intend to use one.

2. Existing Event Sources
You can choose any of the already registered event sources and add them to the custom event log. EventSentry will copy the necessary registry information to the custom event log 1:1. This has the advantage of preserving the message file associations thus avoiding event viewer problems.

To create/assign an event source with a custom event log simply

- Select the custom event log (if not already selected)
- Type the event source name next to Choose Event Source or choose it from the list
- Click Add

Deleting an Event Source
To delete or reassociate an event source with a default event log simply:

- Select the custom event log (if not already selected)
- Select the event source to be removed
- Click Delete

You will then have the opportunity to reassign the event source with one of the default event logs (Application, Security, ...)

5.3.8.2 Monitoring Custom Event Logs
EventSentry can monitor up to 30 custom event logs. From the Custom Event Logs dialog in filter details, select your custom event logs to monitor:
Monitoring custom event logs is no different than monitoring the default event logs except that you have to choose the names of the custom event logs. After you have selected the appropriate custom event logs (on a global basis) you can then configure EventSentry to monitor one or more of these custom logs on a per filter basis.

5.4 Log File Monitoring

EventSentry can monitor any log (flat) file, and process content based on rules you setup. For example, you can store all lines from a log file in your database and/or log selected content to the application event log.
Prerequisites
Similar to monitor event logs, the EventSentry agent will not rescan existing files when it is started. As such, only new lines that are added to the monitor log file(s) will be parsed.

Log File Types
When monitoring files we distinguish between:

- Non-Delimited Log Files
- Delimited Log Files

Log files are monitored in real time, and every time one or more new lines (terminated with a configurable new line character) are added to the log file, they will be processed by EventSentry.

Non-Delimited Log Files
Non-delimited log files are files that do not follow any particular pattern and do not contain delimiters. When consolidating non-delimited files, EventSentry simply stores each row (according to your rules) in the database for later review and archival purposes. Examples of non-delimited log files are the Windows NT Backup log file and debug files generated by development tools.

Non-delimited log files are easiest to configure, but do not allow you to sort or group searches in the web reports.
Delimited Log Files

Delimited log files are files that follow a preset format where every line is made up by a set of fields that are delimited with a common separator, for example a semi-colon. When consolidating delimited log files, EventSentry will store each field separately in the database and allow you to search and display information in a variety of different ways, for example allowing you to group output by a particular field.

Delimited log files require a file definition so that EventSentry knows how to parse each line of the file. Setting up file definitions is straightforward when using one of the pre-defined templates (e.g. IIS, DHCP) but can be more time consuming if you have to monitor a file type for which no definitions exist.

Steps to Monitoring a Log File

1. Delimited Files Only: Create a file definition if none exist
2. Define the monitored file(s)
3. Create & assign a log file package
4. Specify the consolidation and monitoring options

5.4.1 Creating File Definitions

Since delimited log files follow a predefined pattern, you will have to mirror the layout of the delimited log file inside EventSentry, so that EventSentry knows how to parse and split up the log file when it consolidates information to the database. Once a log file definition has been created it can be applied to one or more log files (see next section).

Monitoring delimited log files has the advantage of being able to perform searches and create reports based on the available fields in the log file. For example, if you are monitoring an IIS log file, then you will be able to view most frequently logged remote IP address in a report.

To create a new or edit an existing file definition, right-click the Log File Packages container and select Files and Files Types. The Log File Definitions area will show you all currently configured file definitions and allow you to add new definitions.
To add a new definition, click the Add button which will show the Log File Definition dialog. You can also edit an existing definition by double-clicking a definition from the list. The dialog is divided into two main sections - “General” and “Mappings” - both of which are required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description / Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name for this definition</td>
<td>Firewall Log</td>
</tr>
<tr>
<td>Line Separator</td>
<td>You will almost always want this set to Windows unless you are directly monitoring files on a Unix/Linux machine.</td>
<td></td>
</tr>
<tr>
<td>Field Delimiter</td>
<td>The character by which fields in the log file are separated</td>
<td>;</td>
</tr>
<tr>
<td>Comments start with</td>
<td>Lines starting with the specified character will be ignored</td>
<td>#</td>
</tr>
</tbody>
</table>
Monitoring with EventSentry

Ignore following characters
All the characters specified here will be removed from the current line before it is analyzed.

Skip empty fields
Ignore empty fields, has the same effect as setting individual fields to "Ignore". Using this option may be easier to configure for log files which contain many empty fields.

Merge remaining text
By default, EventSentry will only map fields which are mapped. If the log file contains more fields, they will be ignored. Checking this option will merge any remaining fields and append them to the last mapped field. This is usually only useful for log files which contain a variable number of fields which are rarely used but should still be consolidated.

Timestamps are UTC
Indicates that the time stamp is logged in UTC (opposed to local time).

Prefer US date format
Due to the different date formats in use globally (MM/DD vs DD/MM) it may not always be possible for the agent to detect the date format automatically. If the date format in a log file is in US date format (month before day) it's recommended to check this box.

Mappings
The Mappings section allows you to tell EventSentry what the structure of the log file looks like so that EventSentry can parse the file correctly and map individual fields to their respective data types. Don't be intimated by the number of fields in the dialog, this chapter will explain how to create a new mapping from scratch. Creating a new file definition from scratch can take some time, but keep in mind that it is a one-time process that you will not have to repeat unless you change the layout of the log file.

Using Templates
If a file definition is already listed in the "Load from template" section then you are highly encouraged to select the definition from the pull-down list and click Load to pre-fill the mappings. Once the mappings are displayed, compare them with the log file you are intending to monitor and make sure that the mappings from the temp file match the content of the file. Some applications include a default log format which can be customized, so it is important that you adapt the mappings if the default format has been modified.

The best way to go about mapping a log file is to open the log file up in a spreadsheet application such as Microsoft Excel or OpenOffice Calc. This will allow you to convert the file to fields and easily see each line split into the individual fields. If you do not have a spreadsheet application available, then you can simply open the log file in a text editor such as Notepad.

When you have a clear picture of the available fields in the log file, you can start deciding how to map the individual fields starting from the left. For each of the fields available in the log file, you will perform the following steps:

1. Specify a description of the field
2. Map the field type to one of the available database data types

1. Field Description
Specifying a field description will help you analyze the log file through the EventSentry web reports. Rather than leaving the default "Field XX" description in place, enter a descriptive name of field, for example "Source IP" or "Bytes Transferred". This information will then be shown in the search output and reports. You can find this information either in the header of the log file or the application that is generating the log file.

2. Mapping to a Database Data Type
After you have entered the field description, you can map the field content to a data type. Please see the table below to see which database types are available to be used. Note that only a limited
number of fields are available for each type. For example, once you have used the data type "Integer [#1]" for a field, you cannot use it again will need to use "Integer [#2]" the next time you want to map a field to the integer type.

Please see the table below to see which types are available for use:

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Maximum Length</th>
<th>Maximum Usage Count</th>
<th>Best Use Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore</td>
<td>n/a</td>
<td>unlimited</td>
<td>Use to ignore fields you are not interested in</td>
</tr>
<tr>
<td>Integer</td>
<td>0 - 21474836</td>
<td>18</td>
<td>Use for number fields</td>
</tr>
<tr>
<td>Text (32 chars max)</td>
<td>32 characters</td>
<td>4</td>
<td>Use for short strings that are unique in most lines of the log file</td>
</tr>
<tr>
<td>Text (512 chars max)</td>
<td>512 characters</td>
<td>4</td>
<td>Use for medium-sized strings that are unique in most lines of the log file</td>
</tr>
<tr>
<td>Text (1024 chars max)</td>
<td>1024 characters</td>
<td>2</td>
<td>Use for long strings that are unique in most lines of the log file</td>
</tr>
<tr>
<td>Lookup Text</td>
<td>1024 characters</td>
<td>8</td>
<td>Use for any string that keeps re-appearing throughout the log file</td>
</tr>
<tr>
<td>Date / Time</td>
<td>n/a</td>
<td>2</td>
<td>Use for any string that represents a date / time (see below for more info)</td>
</tr>
</tbody>
</table>

Text or Lookup Text?

While it is probably obvious when to use the "Ignore" and "Integer" field type, it is less obvious as to whether you should use the "Text ..." or "Lookup Text" data type for a text field.

Use this rule: If the text of the field keeps appearing through the log file(s), for example an IP address in a firewall log file, then you should use the "Lookup Text" data type. Text of this type is stored only once in a central lookup table, saving database space and allowing you to group output in the reports by the field. For example, if the field is the IP address of internal hosts from a firewall log file, then you can view a report that shows how many lines from computer have been logged by the firewall!

If, on the other hand, the text of the field is unique for almost every row (e.g. a date or time stamp), then it is best if you assign the text to a regular text type. It wouldn't make sense to fill a lookup table up with values that change millions of times.

Date / Time

Instead of storing timestamps as string values, common date/time formats can be parsed and converted to a timestamp value if either of the following is true for the selected field (column) in the log file:

- The timestamp contains the date and time
- The timestamp contains only the date but the field immediately following the date contains the time (see screen shot below)

If the column of a log file that is marked as Date / Time only contains a date (without the time), then EventSentry will fetch the time from the next column by merging the two columns. As such, if a log file logs the date & time in separate columns, only a single Date / Time definition is needed.
Parsing only a date (e.g. 12/1/2019) or only a time (e.g. 15:03:44) is not supported; incomplete date strings require a text-style field type (text or lookup text).

The screen shot below shows a log file where date and time are split into two columns, the matching log file definition is shown below:
5.4.2 Defining Monitored Files

Once you have created a file definition for your delimited file, or, if you are monitoring non-delimited files, you can configure the actual files that are to be monitored. EventSentry supports variables and wildcards for log files that include dynamic strings such as date, time and sequence numbers.

When adding a new file, you will be required to point to the path of the log file (variables and wildcards are supported), enter a unique name for the log file and specify whether the file is delimited (including a file type) or non-delimited.

To create a new or edit an existing file definition, right-click the Log File Packages container and select Files and Files Types. The Files area will show you all currently configured files and allow you to specify new files.

Monitoring a new log file

Click the Add button to bring up the Add / Edit File to Monitor dialog.

Add / Edit File to Monitor

Enter a descriptive name for this file (you will refer to this file under this name), select a file definition (or choose “Non-Delimited”) and specify the path to the file. Simple file definitions require less setup but will occupy significantly more space in the database.

Name:
Specify a descriptive name for the log file. For example, enter Firewall Log File if you are monitoring the log file of your firewall.

File Definition
If you are monitoring a non-delimited file, check the Non-Delimited checkbox. Otherwise, select the file definition from the pull-down menu. If a suitable definition is not in the list, then you will have to create a new file definition.

Path
Specify the full path to the log file. Since log files usually include dynamic strings such as the current date, file etc., you can include variables and/or wildcards in the path name. The following variables and wildcards are supported:

<table>
<thead>
<tr>
<th>Character/Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Wildcard</td>
<td>matches zero or more characters</td>
</tr>
<tr>
<td>?</td>
<td>Wildcard</td>
<td>matches a single character</td>
</tr>
<tr>
<td>$YEAR</td>
<td>Variable</td>
<td>4-digit year</td>
</tr>
</tbody>
</table>

By default, the Windows Update client records all transaction information to this file.

Name: Windows Update Log
File Definition: Non-Delimited
Path: C:\Windows\WindowsUpdate.log
Since you can use both wildcards and variables, you can often specify the file name of your log files in two different ways - either with using wildcards or by using variables. See the table below for examples on how to map file names:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Filename</th>
<th>Filename</th>
<th>$YEARSHORT $MONTH $DAY.log</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntbackup01.log</td>
<td>ex070501.log</td>
<td>ex070501.log</td>
<td>2007011023233 Mar 15, 2007</td>
</tr>
<tr>
<td>ntbackup02.log</td>
<td>ex070502.log</td>
<td>ex070502.log</td>
<td>20070340242343 Mar 16, 2007</td>
</tr>
<tr>
<td>ntbackup03.log</td>
<td>ex070503.log</td>
<td>ex070503.log</td>
<td>20070139619433 Mar 15, 2007</td>
</tr>
<tr>
<td>ntbackup*.log</td>
<td>ex$YEARSHORT$MONTH$DAY.log</td>
<td>ex*.log</td>
<td>SYEAR*$DAY, $YEAR*.txt</td>
</tr>
</tbody>
</table>

As can be seen from the 2nd and 3rd column, the log file name can sometimes be specified in different ways.

**Include Subdirectories**

File in sub directories can be monitored by checking this box. When monitoring files in sub directories, the path can be specified in a variety of ways:

<table>
<thead>
<tr>
<th>Path</th>
<th>$PATH$</th>
<th>Files Monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\LogFiles*.log</td>
<td>Monitors all files with the .log extension in the C:\LogFiles folder as well as sub directories</td>
<td></td>
</tr>
<tr>
<td>C:\LogFiles*.log</td>
<td>Monitors all files with the .log extension in any sub directory of the C:\LogFiles folder (and not in the main C:\LogFiles folder)</td>
<td></td>
</tr>
<tr>
<td>C:\inetpub\logs\LogFiles\W3SVC*\u_*.log</td>
<td>Monitors all files which match the u_<em>.log pattern in any sub directory of C:\inetpub\logs\LogFiles which matches the W3SVC</em> pattern</td>
<td></td>
</tr>
</tbody>
</table>

**Notes**

You can use notes to specify what application generates the log file or other descriptions.

### 5.4.3 Adding Files to a Log File Package

A log file package contains one or more monitored files, and can be assigned to globally or to individual computers or groups. To create a new log file package, right-click the Log File Packages container, select Add Package and enter a name for the new package.

To add a file to this package, right-click the log file package and select Add File. This will show the "Select File to Monitor" dialog that shows all the files that can be added to this log file package. Files that are already contained in the log file package will not be shown in the dialog. To add a file, select it and click the OK button.
The selected file will appear under the log file package it was added to, and can be edited by clicking the file name.

Removing or disabling log files
To remove a file from being monitored, right-click the file under the log file package and select “Delete”. This will remove the file from the selected package. You can also right-click the package and select “Disable” to prevent the file from being monitored.

5.4.4 Consolidation & Monitoring Options
Once a file has been added to a package, you will have to instruct EventSentry what to do with its content. You can either consolidate lines from the log file to a database, log the text to the application event log, or both. In addition, EventSentry allows you to include or exclude lines based on the keywords.

Storing Log Files in a Database
To consolidate content from log files in a database, click the “Database Consolidation” tab and select a database destination from the “Destination” section by clicking the “Add” button. You can specify up to four different databases.

By default, all lines parsed from the log file will be sent to the specified database(s). To change this behavior, you can either exclude certain lines from being added to the database (include all, exclude some), or only send specific lines to the database. Click the + icon to add strings that will trigger the database.

Include: Log all lines to the database, except for exclusions below
This is the default setting, and it will send all parsed lines from the log file to the database. Lines in the log file containing strings that are listed below will not be sent to the database. This allows you to conserve space in the database if your log file contains unneeded content.
Exclude: Only log lines to the database that are included below
This setting is more restrictive and will only send lines from the log file to that database that are listed below. This allows you to only send content to the database that matches your filters. For example, you can only send lines that contain "Error" or "Warning" to the database to aid troubleshooting.

Load
Loads filter rules from a text file (one entry per line) and appends them to the current list of filters.

Logging lines from the log file to the event log
To log lines from log files to the application event log, click the "Event Log Alerts" tab and check the "Log to APPLICATION Event Log" check box. You can also select the severity under which entries in the event log are written as.

Context
When a matching line in a log file is found, the alert can contain up to 5 lines before and after of the matching line to provide context. Set to “None” to disable the log context feature.

By default, no lines parsed from the log file will be logged to the event log. Click the + icon to add strings that will trigger event log alerts.

Include: Log all lines to the event log, except for exclusions below
This setting will log all parsed lines from the log file to the event log. Lines in the log file containing strings that are listed below will not be logged to the event log. This setting is not recommended as it can quickly fill the application event log.

Exclude: Only log lines to the database that are included below
This is the default setting, and will log lines from the log file to the event log that match the strings listed below. This allows you to only send content to the event log that matches your filters. For example, you can only log lines that contain "Error" or "Warning" to the event log to aid troubleshooting.

Load
Loads filter rules from a text file (one entry per line) and appends them to the current list of filters.

Text Match Type
Specifies whether text matching uses simple wild card matching or regex pattern matching.

5.4.4.1 Event Logs
The following event log records are be logged by this feature with the Log File Monitoring category:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>8000</td>
<td>Text matching one or more filter rules has been found.</td>
<td>Text matching one or more filter rules has been found in file C:\Logs\ntbackup01.log:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Line in monitored file</td>
</tr>
<tr>
<td>8001</td>
<td>EventSentry is caching more than 1024 files in the monitored directory C:\Logs.</td>
<td>EventSentry is caching more than 1024 files in the monitored directory C:\Logs. To keep the resource consumption of the EventSentry agent low it is recommended that you move old files to a sub directory or another directory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A line in the previously monitored file C:\Logs\ntbackup01.log did not contain a CRLF and as such was not processed according to the filter rule. The line from the text file is shown below:</td>
</tr>
<tr>
<td>8002</td>
<td>A line did not contain a CRLF.</td>
<td>A line in the previously monitored file C:\Logs\ntbackup01.log did not contain a CRLF and as such was not processed according to the filter rule. The line from the text file is shown below:</td>
</tr>
</tbody>
</table>

© <2002 - 2022> ... NETIKUS.NET ltd
5.5 System Health Monitoring

EventSentry can monitor several metrics of the Operating System to detect potential failures and problems as well as provide a searchable interface to key objects. With System Health Monitoring EventSentry can generate alerts in the application event log and/or consolidate information (e.g. CPU usage history, installed applications) in a central database.

Overview

You can monitor the following system objects:

- Services
- Monitor and track any performance counter
- Monitor the memory usage of processes to detect faulty applications with memory leaks
- Monitor whether certain processes are active
- Monitor and recording disk space
- Monitor selected directories
- Monitor certain registry keys and file locations to detect if applications are installed/uninstalled or if an application registers itself to be automatically started when a user logs in
- Monitor directories for file size changes, file additions/deletions and file checksum changes
- Ensure time is synchronized with a NTP server
- Scheduled Tasks

Additionally you can

- Launch command-line applications at defined schedules and have their output logged to the event log
- Backup and clear event logs at defined schedules
- Control Services
- Utilize a system tray application

All alerts generated by a system health feature (e.g. service status change, low disk space alert, performance alert) will be logged to the Application event log.

As such, the application event log will need to be monitored with at least one event log filter (this is enabled by default). In addition, every system health dialog includes an "Alerts ..." button which launches a wizard that will create the necessary event log filter.

Built-In System Health Packages

NETIKUS.NET maintains a set of health packages that contain common health settings for service, disk space and performance monitoring. These event log packages are installed automatically with EventSentry and can be updated automatically over the Internet. See Downloading Packages for more information.

Adding/Removing health objects to a Health Package
A health package consists of one or more health objects, whereas every monitoring feature (service monitoring, performance monitoring, etc.) is a health object that can be added to a health package.

To add a health object to a health package, right-click the health package and select the desired health object from the Add submenu:

The new health object will appear under the health package with a blue wheel icon associated with it. Please note that you cannot add more than one health object of the same type to the same health package. For example, you cannot add two Service Monitoring objects to the same health object.

To remove a health monitoring object, right-click the health object and select Remove this object.

5.5.1 Alerts

Almost all system health objects store data in the EventSentry database but can also generate alerts (e.g. disk space is low) that are written to the event log. See the table below for more information on which features report to the database and/or generate alerts. Each feature can be configured individually and alerts can be either enabled or disabled.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Database Alerts</th>
<th>Alerts Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Monitoring</td>
<td>Yes Yes</td>
<td>When services or drivers are added, removed or change status.</td>
</tr>
<tr>
<td>Application Scheduler</td>
<td>No Yes</td>
<td>Process output (when configured) or when errors occurred.</td>
</tr>
<tr>
<td>Backup Event Logs</td>
<td>No Yes</td>
<td>When event log backups etc have completed or when errors occurred.</td>
</tr>
<tr>
<td>Process Monitoring</td>
<td>Yes Yes</td>
<td>When critical processes are inactive, or new processes are accepting network connections.</td>
</tr>
<tr>
<td>Disk Space Monitoring</td>
<td>Yes Yes</td>
<td>When disk space is low.</td>
</tr>
<tr>
<td>Directory Monitoring</td>
<td>Yes Yes</td>
<td>When directory size or file count exceeds limits.</td>
</tr>
<tr>
<td>Software / Hardware Monitoring</td>
<td>Yes Yes</td>
<td>When software/browser extensions are added/removed, when BIOS or installed memory change</td>
</tr>
<tr>
<td>Performance Monitoring</td>
<td>Yes Yes</td>
<td>When performance counters exceed limits.</td>
</tr>
</tbody>
</table>
To maintain consistency and retain a log of all alerts generated by a system health feature, all alerts are written to the event log. Please see the respective “Event Log” sub chapter of each feature.

In order to get notifications (e.g. email) of system health alerts, event log filters will need to dispatch these alerts to the appropriate action. Many alerts generated by system health features are logged with an Error severity, which ensures that they are automatically picked up by default email filter rules. Severities can be changed however, which is why it is important to understand the architecture and flow of events.

The diagram below illustrates how each feature logs alerts to event log, which are then analyzed and, upon matching, dispatched to one or more actions.

### 5.5.2 Service Monitoring

Service monitoring offers the following features:

- Detect service status changes (stopped -> running, paused -> stopped, etc.)
- Detect if services are added or removed
- Detect service configuration changes (service account change, executable change)
- Detect if a service set to auto-start did not start
- Ensure that a service is always in a desired state (stopped or running)
- Track service status, changes and activity in a database
Service Monitoring is supported on Unix/Linux hosts when SSH credentials are configured. Service monitoring alerts are identical between Windows and Non-Windows hosts but generally contain more details on Windows.

Service data on Non-Windows hosts is collected by the Heartbeat Agent.

### Service & Driver Monitoring

This component can be configured to either monitor all services, only specific services or no services.

- **Monitor all Services:** All services, except the ones included in the listbox, are monitored.
- **Monitor only Selected Services:** Only the services shown in the list box are monitored. If the list box is empty then service monitoring will not be active.
- **Do not monitor services:** No services are monitored, and all services from the list box are removed.

If the Boot Time Behavior is set to "Rescan after Reboot", then service status changes will also be monitored during reboots and/or EventSentry service restarts. For example, if the Server Service status was running when you stop the EventSentry service, but stopped when you started the EventSentry service, then this status change will be logged.

Services are displayed with both the display name and the service key name in the list. If a service is a driver then Yes will be shown in the Driver column, otherwise No.

### Adding and Removing Services from the List

Clicking the plus (+) button on the right of the list adds a service to the list of monitored (or excluded) services. The dialog displayed when clicking the plus button will allow you to choose a service (or driver) from a drop-down list to add to the list. Please note that services starting with an asterisk (*) indicate that this service is a driver. Drivers will only be shown in this list if you check the Monitor Drivers check box. Partial service names using wild cards (e.g. sql*) are supported.

If a service specified in this list does not exist on a remote host, it will simply be ignored - no warning will be issued.
A service can be removed by selecting it in the list and clicking the minus (-) button.

You can also add services which are not listed in the “Service Display Name” list by entering the service name. This can be the case if a service is installed on a monitored server but not on the management server. Partial service names using wildcards are supported.

**Monitoring Interval**
Services are monitored every 10 seconds. When a service change is detected, the service monitoring interval is temporarily reduced to 5 seconds for one minute.

**What to Monitor**
Service Monitoring can monitor services status changes, changes in the SCM (=Service Control Manager) database, or both. Monitoring drivers is configurable.

- **Monitor Status Changes**: If the status of a service changes, then an event in the Application event log will be generated. For example, if the Messenger service is stopped, EventSentry will indicate that the Messenger changed from Running to Stopped.

- **When service is stopped, notify every**: When checked, additionally generates continuous alerts when a service remains in the “Stopped” state for the specified time period.

- **Monitor SCM Changes**: If a service is added or removed, EventSentry will log an event in the Application event log.

- **Monitor Drivers**: Select this option to monitor drivers.

- **Log Changes As** configures the severity with which events are written to the Application event log.

- **Record in database** configures whether this component records activity in a database (action).
Advanced Options
See “Advanced Options” for more details.

Force Service Status
Ensures that certain services are always in a Running or Stopped state (individually configurable per service).

To control a service, click the + button and select a service from the list. If the requested service is not in the list you may simply type the service key name into the “Service Display Name” field. Then specify the desire service state (e.g. "Running") and click the OK button. EventSentry will now make sure that the service is always in the requested state.

In the example below, the Windows Firewall service (service key name MpsSvc) will be started if it is stopped.

Whenever the agent determines that a service is not in the requested state it will attempt to change the state accordingly and write a message to the event log unless the host is in a maintenance schedule. The Log Service Control Attempts As setting determines the severity with which these messages are written to the event log.

A maintenance schedule can be assigned to a host in order to temporarily change the status of a service. The Service Status Control feature is inactive while a host is in maintenance schedule.

Limitations
If a service status is changed twice during a monitoring interval, then the status change cannot be detected by EventSentry, this is extremely unlikely to happen however.

Implications on System Load
Service monitoring does not have a high impact on the system load.

5.5.2.1 Advanced Options
On Startup, check if services set to AUTO are running
You can automatically verify that all services that are set to automatically start with Windows are actually running. It is recommended to also set a startup delay (Start monitoring ...) when activating this feature. Many services and drivers (started after or with EventSentry) are not yet running when EventSentry is started, but will be running a few minutes after. Setting the delay depends on the hardware, the OS you are using and the number of services you are monitoring. The recommended default is 120 seconds.
5.5.2.2 Linux / Unix Configuration

In order to utilize the "Force Service Status" feature on Unix/Linux operating systems, additional configuration steps may be necessary for security reasons. The steps below are not necessary if the target system you are monitoring allows root logins via SSH, and the account configured in EventSentry is the root user or equivalent.

The instructions below should work on most common Linux distributions but may differ and come without warranty. On the target systems perform the following steps.

1. Create a new user by running this command:

   `sudo useradd -m [username]`

2. Create a password for the new user (write down the user name and password since that will later need to be configured in EventSentry):

   `sudo passwd [username]`

3. Grant the new user access to the command to start/stop services. This requires the creation of a file in `/etc/sudoers.d` called `[username]`. You can use your preferred text editor, for this example we use `nano`.

   The `sudoers` file is a critical and sensitive file; a typo or an error in this file could lead to issues executing elevated commands and render the system unusable. Double check before saving.

   `sudo nano /etc/sudoers.d/[username]`

   The following 3 lines must be added to this new file:

   ```
   [username] ALL=NOPASSWD: /bin/systemctl start *
   [username] ALL=NOPASSWD: /bin/systemctl stop *
   [username] ALL=NOPASSWD: /bin/systemctl status *
   ```

   Replace `[username]` with the username that was enter in step 1. Save the changes by using CTRL+S and exit the editor with CTRL+X.

   An alternative way to do the same is by downloading our creation script and run it by:


   `sudo sh es_servicemonitor.sh`

   The script will ask for the username and password and will create the corresponding files authorize that user to start/stop services.
### Event Log

The following events are logged by this feature with the **Service Monitoring** event category. The top event ID is logged when activity with a service is detected, the bottom event ID is logged when activity with a driver is detected.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| 1010 0   | A service status changed | The status for service BITS (Background Intelligent Transfer Service) changed from Start Pending to Running. Additional Service Information:  
Startup type: Automatic  
Executable: C:\WINDOWS\system32\svchost.exe -k netsvcs  
Service account: LocalSystem |
| 1015 0   |                       |         |
| 1010 1   | A service was added  | A service was added:  
Additional Service Information:  
Name: GatewayIPMonitor (Gateway IP Monitor)  
Status: Running  
Startup type: Automatic  
Executable: C:\Program Files (x86)\Gateway IP Monitor\gwipmon_svc.exe  
Service Account: LocalSystem |
| 1015 1   |                       |         |
| 1010 2   | A service was removed | A service was removed: GatewayIPMonitor (Gateway IP Monitor).  
Additional Service Information:  
Status: Running  
Startup type: Automatic  
Executable: C:\Program Files (x86)\Gateway IP Monitor\gwipmon_svc.exe  
Service Account: LocalSystem |
| 1015 2   |                       |         |
| 1010 3   | A service is being monitored | The service EventSentry (EventSentry) is now being monitored.  
Additional Service Information:  
Status: Running  
Startup type: Automatic  
Executable: C:\Program Files (x86)\Gateway IP Monitor\gwipmon_svc.exe  
Service Account: LocalSystem |
<p>| 1015 3   |                       |         |
| 1010 4   | A service is not being monitored anymore | The service Cdaudio (Cdaudio) will not be monitored anymore. Last service status was Stopped. |
| 1015 4   |                       |         |</p>
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10105</td>
<td>Services configured for autostart are not running</td>
<td>The following 3 service(s) are configured to AUTOSTART but are currently not running: Cdaudio Digital CD Audio Playback Filter Driver Sfloppy</td>
</tr>
<tr>
<td>10106</td>
<td>Unable to connect to SCM</td>
<td>Unable to connect to the Service Control Manager (SCM), services cannot be monitored.</td>
</tr>
<tr>
<td>10107</td>
<td>Unable to enumerate services</td>
<td>Unable to enumerate services, services cannot be monitored.</td>
</tr>
<tr>
<td>10108</td>
<td>Successfully changed service state</td>
<td>The state of service USB Mass Storage Driver was Running, requested state is Stopped. EventSentry successfully changed the service status to Stopped.</td>
</tr>
<tr>
<td>10109</td>
<td>Unable to change service state</td>
<td>The state of service iPodService is Start Pending, requested state is Stopped. EventSentry was not able to change the service status due to the following error: The service is pending stop.</td>
</tr>
<tr>
<td>10110</td>
<td>A service startup type changed</td>
<td>The Startup Type for service dcevt64 (DSM SA Event Manager) changed from Automatic to Manual.</td>
</tr>
<tr>
<td></td>
<td>Additional Service Information:</td>
<td>Status: Running</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Startup type: Automatic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Executable: &quot;C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service Account: LocalSystem</td>
</tr>
<tr>
<td>10111</td>
<td>The user account for a service changed</td>
<td>The user account for service dcevt64 (DSM SA Event Manager) changed from LocalSystem to DellServiceAccount.</td>
</tr>
<tr>
<td></td>
<td>Additional Service Information:</td>
<td>Status: Running</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Startup type: Automatic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Executable: &quot;C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe&quot;</td>
</tr>
<tr>
<td>10112</td>
<td>The executable for a service changed</td>
<td>The executable for service dcevt64 (DSM SA Event Manager) changed from &quot;C:\Program Files (x86) \Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr.exe&quot; to &quot;C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe&quot;</td>
</tr>
<tr>
<td></td>
<td>Additional Service Information:</td>
<td>Status: Running</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Startup type: Automatic</td>
</tr>
<tr>
<td>1011 4</td>
<td>A service remains stopped</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>1016 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The status for service dcevt64 (DSM SA Event Manager) remains stopped.

Additional Service Information:

- Startup type: Automatic
- Executable: "C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe"
- Service Account: LocalSystem
A Service Status changed and is logged to the Event Log
5.5.3 Application Scheduler

Schedule any (command-line) application from within EventSentry for custom system monitoring and task automation. Support batch files, executables and any script language (e.g. PowerShell, Perl, Visual Basic Script, ...) for which an interpreter is installed.

In addition to scheduling applications & scripts at set date and times, also supports continuously schedules every X minutes. The agent logs the output of the application to the event log with a dynamic severity (information or error) which supports error handling and automated remediation utilizing event log filters. See Event Logs for all possible event log records logged by this feature.

Executables launched with this feature will run under the same security account that the EventSentry agent is running under, the LocalSystem account by default. Take this into consideration when intending to run applications that require access to resources located on the network.

Embedded Scripts

The application scheduler can either launch existing scripts that are present on the host, or launch an embedded script.

Process and/or scripts launched by the application scheduler feature which display message boxes, license dialogs and similar will not work as they will indefinitely block. For example, this affects some of the Sysinternals utilities which tend to display a license dialog the first time they are run.

Scheduling an application to run at set date/time

To schedule an application to run at a preset date and time, for example every day at 3pm, click the plus button next to the schedule list. You will be presented with the following dialog:
Set the **Schedule Type** to "Regular Schedule", and in the **Date & Time** area schedule the application to either run on certain weekdays, on certain days of the month or both.

The **Process Timeout** feature allows you to terminate a process if it runs longer than a certain amount of minutes. Set this option to 0 (minutes) to let processes run until they terminate on their own.

Specify the file to be executed in the **Filename** field. You can either specify or select an existing script with the “Browse” button, or select an [embedded script](#) with the drop-down menu. Embedded scripts are specified with the @ symbol in front of the file, as shown in the screenshot above.

When **Terminate child processes** is checked, then all child processes that have been launched by **Filename** will be terminated recursively.

**Scheduling an application to run periodically**

To schedule an application to run continuously, for example every 5 minutes, click the **plus** button next to the schedule list. You will be presented with the following dialog:
Set the Schedule Type to "Recurring Schedule" and configure it accordingly. The schedule can be restricted further by only having the application run during certain time periods, for example between 8AM and 5PM.

**Changing an Existing Schedule**
You can change existing schedules by double-clicking on the entries in the schedule list.

When launching a script (e.g. VBScript), then it is recommended that point the Filename field to the scripting engine (e.g. cscript.exe) with the script file as the argument. For example:

```
c:\windows\system32\cscript.exe c:\batch\files_count.vbs
```

to execute the file `c:\batch\files_count.vbs`.

**Application Return Codes**
To take advantage of the return code analysis, it is recommend to either call executable applications directly (e.g. ping.exe) or to invoke scripts using a scripting engine that let you specify the return code (e.g. VBScript using cscript.exe). It is not recommended that you use batch files if the application return code is of significance.

- Checking the "Log application return code 0 to event log", will log an information event to the application event log, showing the text output of the script.
• Checking the “Log application return code > 0 to event log”, will log an error to the application event log, showing the text output of the script.

The next chapter, “Example Scripts”, lists Visual Basic scripts that would work well with the Application Scheduler feature.

5.5.3.1 Example Scripts

The following scripts can be used by the applications scheduler and will return an error code depending on whether they ran successfully or not. Variables that need to be adjusted are highlighted in green below. All examples below use Visual Basic Script. Additional example scripts are available in the Scripts sub folder of the EventSentry installation directory.

This script counts the number of files in a folder and can return 1 if the number of files exceeds a threshold.

```
' ----------------------
' --- file_count.vbs ---
' ----------------------
' Counts the number of files in a folder (without traversing subfolders)
'
' Returns 1 if the number of files is larger than MyLimit or 0 if the number of files is equal or less than MyLimit

Dim FS, FO, FC
Dim MyFolder, MyLimit

' Set your values here
MyFolder   = "C:\Batch"
MyLimit    = 200

Set FS = CreateObject("Scripting.FileSystemObject")
Set FO = FS.GetFolder(MyFolder)
Set FC = FO.Files

WScript.Echo "Folder " & MyFolder & " contains " & FC.Count & " files."

If FC.Count > MyLimit Then
    WScript.Quit(1)
Else
    WScript.Quit(0)
End If
```

This script enumerates all fans in the system that can be monitored through WMI (if supported). If one or more of the monitored fans report a status other than "Other", "Unknown" or "Running", then the script will return 1.

```
' --------------------------
' --- system_faninfo.vbs ---
' --------------------------
On Error Resume Next
Dim GlobalError

GlobalError = 0
```
Function ExplainAvailability(Availability)
    Select Case Availability
        Case 1: ExplainAvailability = "Other"
        Case 2: ExplainAvailability = "Unknown"
        Case 3: ExplainAvailability = "Running / Full Power"
        Case 4: ExplainAvailability = "Warning"
        Case 5: ExplainAvailability = "In Test"
        Case 6: ExplainAvailability = "Not Applicable"
        Case 7: ExplainAvailability = "Power Off"
        Case 8: ExplainAvailability = "Off Line"
        Case 9: ExplainAvailability = "Off Duty"
        Case 10: ExplainAvailability = "Degraded"
        Case 11: ExplainAvailability = "Not Installed"
        Case 12: ExplainAvailability = "Install Error"
        Case 13: ExplainAvailability = "Power Save – Unknown"
        Case 14: ExplainAvailability = "Power Save – Low Power Mode"
        Case 15: ExplainAvailability = "Power Save – Standby"
        Case 16: ExplainAvailability = "Power Cycle"
        Case 17: ExplainAvailability = "Power Save – Warning"
    End Select
End Function

Function ExplainStatus(Status)
    Select Case Status
        Case 1: ExplainStatus = "Other"
        Case 2: ExplainStatus = "Unknown"
        Case 3: ExplainStatus = "Enabled"
        Case 4: ExplainStatus = "Disabled"
        Case 5: ExplainStatus = "Not Applicable"
    End Select
End Function

strComputer = "."
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate)!\" & strComputer & "\root\cimv2")
Set colItems = objWMIService.ExecQuery("Select * from Win32_Fan")
For Each objItem in colItems
    Wscript.Echo "Name:           " & objItem.Name
    Wscript.Echo "Active Cooling: " & objItem.ActiveCooling
    Wscript.Echo "Availability:   " & ExplainAvailability(objItem.Availability) & " (" & objItem.Availability & ")"
    Wscript.Echo "Device ID:      " & objItem.DeviceID
Next
' Analyze
If objItem.Availability > 3 Then
    GlobalError = 1
End If
Wscript.Quit(GlobalError)
## Event Log

The following events are logged by this feature with the **Application Scheduler** event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10200</td>
<td>An application was executed successfully.</td>
<td>superdel.exe was run for 15 seconds with the result shown below. Return Code was 0.</td>
</tr>
<tr>
<td>10201</td>
<td>A process could not be created.</td>
<td>The process superdel.exe could not be created due to the following error: The file could not be found.</td>
</tr>
<tr>
<td>10202</td>
<td>A process exceeded the maximum configured time interval, but the process could not be terminated.</td>
<td>The process superdel.exe exceeded the maximum allowed time interval of 15 minute(s). EventSentry was unable to terminate the process due to the following error: Access Denied.</td>
</tr>
<tr>
<td>10203</td>
<td>A process exceeded the maximum configured time interval and was terminated.</td>
<td>The process superdel.exe exceeded the maximum allowed time interval of 15 minute(s). The process was terminated. Please increase the timeout interval for this drive in the management application (System Health -&gt; 3rd Party Applications).</td>
</tr>
<tr>
<td>10204</td>
<td>A process was executed successfully.</td>
<td>dosomething.exe was executed successfully.</td>
</tr>
<tr>
<td>10205</td>
<td>A process exceeded the maximum configured time interval but could not be terminated. 0 or more child processes were terminated.</td>
<td>The process dosomething.exe exceeded the maximum allowed time interval of 2 minute(s). EventSentry was unable to terminate the process due to the following error: Access Denied 1 child process(es) were successfully terminated.</td>
</tr>
<tr>
<td>10206</td>
<td>A process exceeded the maximum configured time interval and was terminated.</td>
<td>The process adlist.exe exceeded the maximum allowed time interval of 5 minute(s). The process and 0 child process(es) was terminated. Please increase the timeout interval for this process in the management console (System Health -&gt; Application Scheduler).</td>
</tr>
<tr>
<td>10210</td>
<td>A process was not started because the isolation level of the schedule is set to local and another instance of the same script is already running.</td>
<td>The process adlist.exe was not started because the script is configured for local isolation and another instance of the same script is already running.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Error Message</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>10211</td>
<td>A process wasn't started because it is configured for global isolation, and another process also configured for global isolation is already running.</td>
<td></td>
</tr>
<tr>
<td>5.5.4</td>
<td>Backup Event Logs</td>
<td></td>
</tr>
</tbody>
</table>

Backing up and/or clearing event logs can be scheduled to run at specified intervals, results are always logged to the event log. Alerts can also be triggered when an event log is full.

If you encounter problems when backing up and clearing the event logs then please see KB article 21 for a solution to common problems.

The screenshot below shows an existing schedule that backs up the Application event log every Monday at 5am. The event log is not cleared, and the results are logged to the event log.

To add a new schedule click on the + button next to the schedule list, to edit an existing entry simple double-click the entry:
Event Log

Either select the event log to backup/clear from the pull down menu or specify the log name manually. To backup all event logs on the computer specify the "All Event Logs" option.

Date & Time

Schedules the backup/clearing to either run on certain weekdays, on certain days of the month or both.

Backup

Specifying a file name in the "File" section will cause the "Backup Event Log" check box to be automatically checked; the event log will be backed up to the specified file. We recommend that you use the .evtx extension for the file name to avoid confusion. The following case sensitive variables are supported in the file name: $HOSTNAME, $LOG, $DAY, $MONTH, $YEAR, $HOUR, $MINUTE. Compressed files will have the same name as the backup file with the .zip extension appended to them.

Clear Event Log

Checking the "Clear Event Log" check box will clear an event log. The event log may be cleared after it has been backed up (if you specified a file name), or it may be cleared log without it being backed up.

Compress

Since Event Log Backup files can be rather large (depending on the size of your event log) and compress well, you can automatically compress the backed up event log backup files with EventSentry. Compressed files will have the same name as the backup file with the .zip extension appended to them. For example, if the event log backup file name is SRV01_Security_20070808.evt then the name of the archive will be SRV01_Security_20070808.evt.zip.
Checking this box will automatically compress the event log backup file after it has been backed up, and the uncompressed version will be deleted. The size of compressed event log backup files is usually only about 20% (or less) of their original file size.

Since event log backup files are compressed with the ZIP algorithm, they can be extracted/uncompressed with all major compression software, such as 7-Zip.

Log Action(s) to Event Log
To log a history of all backup and clear actions to the event log, activate the “Log action(s) to event log” checkbox. See Event Logs for all possible event log records logged by this feature.

5.5.4.1 Detecting Full Event Logs
If you are running Windows 2000 or higher then you can be notified if an event log is full.

All event logs monitored by your filters will be checked in the interval (must be multiple of 10 seconds) you specify. If a particular event log is full then the specified Smtp action will be notified. No messages will be written to the event logs. An email with the following text will be sent:

The event log Security is full. Please increase the size of the event log or clear the eventlog. Please note that this is an email-only message that will not appear in the Application event log or in other targets.

5.5.4.2 Event Log
The following events are logged by this feature with the Event Log Backup/Clear event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10300</td>
<td>An event log was cleared.</td>
<td>The Application event log was successfully cleared.</td>
</tr>
<tr>
<td>10301</td>
<td>An event log was successfully backed up.</td>
<td>Event log was successfully backed up:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event log: Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File: d:\eventlogs\srv01_app_20120329.evtx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File size: 512000 kBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checksum: 9036E4F5137D957BF0E99176F9C062CE863540D243F7C59 4E1F54213C4BB259C</td>
</tr>
<tr>
<td>10302</td>
<td>An event log was successfully cleared and backed up.</td>
<td>Event log was successfully backed up and cleared:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event log: Application</td>
</tr>
</tbody>
</table>
File: d:\eventlogs\srv01_app_20120329.evtx
File size: 512000 kBytes
Checksum:
9036E4F5137D957BF0E99176F9C062CE863540D243F7C594E1F54213C4BB259C

10303 An event log could not be cleared due to an error.
The Security event log could not be cleared due to the following error: Access is Denied.

10304 An event log could not be backed up due to an error.
The Security event log could not be backed up due to the following error: Access is Denied.

10305 An event log could not be cleared and backed up due to an error.
The System event log could not be cleared and backed up due to the following error: Access is Denied.

10306 The event log backup file "%1" could not be compressed due to the following error:
The event log backup file "C:\Logs\SRV01_Application_20070823.evt" could not be compressed due to the following error: Insufficient Memory.

10307 The event log backup file "%1" appears to have been compressed successfully, but the compressed event log backup file "%2" could not be verified. The original event log backup file will not be deleted.
The event log backup file "C:\Logs\SRV01_Application_20070823.evt" appears to have been compressed successfully, but the compressed event log backup file "C:\Logs\SRV01_Application_20070823.evt.zip" could not be verified. The original event log backup file will not be deleted.

10320 Full event logs cannot be detected.
Full event logs cannot be detected on this machine, this feature is not supported on this platform (only Windows 2000 or higher).

5.5.5 Process Monitoring

Process monitoring detects when a required processes is inactive and can evaluate the command line parameters of a process. The minimum number of required instances of a process may be specified as well.

Process Monitoring can also alert on inactive processes from a remote SNMP agent by polling SNMP counter values. Process monitoring alerts are identical between Windows and Non-Windows hosts.

SNMP data is collected by the Heartbeat Agent.

Process Monitoring
Monitoring a process
To monitor a process, click the + button and specify the process name as well as the number of required instances (default is "1"). Wildcards can be specified for the process name, e.g. "java*" would match all processes starting with "java".

Command Line Parameters
If only processes with specific command-line parameters should be evaluated, then the required command line can be specified as well. If a command line is not specified, then it will be ignored. This parameter supports wildcards as well.

Process Network Status (aka Netstat)
Enumerates all processes which have an active TCP network connection and makes that information available in the web reports, it provides the same data as the built-in netstat command. If "Detect Changes" is selected, optionally also generates an alert when a process starts listening on a previously inactive TCP connection and vice versa.

The following options are available:

- **Enabled (All Connections):** Enumerates all processes which have an active TCP network connection, including both client-side and server-side processes.
- **Enabled (Listening Ports Only):** Enumerates all processes which are listening for incoming TCP requests, usually server-side processes like web servers, database servers and such.
- **Disabled**

**Detect Changes**
Detected when a previously closed TCP port is in the active listening state, or when a TCP port that was previously listening is now closed. Events are logged with the event severity selected in the Options below.

**Interval**
Determines how often the process state is refreshed.

**Database**
Sets the database where the process data is stored.
The Process Network Status feature is only available on Windows-based hosts.

Options
The severity with which an event is written to the event log can be adjusted by changing the "log errors as" option below the list. When a specified process is not active, event 10401 is logged to the event log once. When the process becomes active again event 10402 will be logged to the application event log (see also Event Log).

To avoid false positives during system boot, adjust the start-up delay accordingly. Simply set the "Start monitoring processes" option to the number of seconds it takes for all processes to be active.

"Notify at most once every" sets how often an alert is generated when the required process(es) is not active.

5.5.5.1 Event Log

The following events are be logged by this feature with the Process Monitoring event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10401</td>
<td>%2 instance(s) of process &quot;%1&quot; on host %4 are active, but %3 instance(s) is/are required.</td>
<td>0 instance(s) of process &quot;eventsentry_gui.exe&quot; on host server14 are active, but 1 instance(s) is/are required.</td>
</tr>
<tr>
<td>10402</td>
<td>%2 instances of process &quot;%1&quot; is/are currently active on host %3.</td>
<td>1 instances of process &quot;eventsentry_gui.exe&quot; is/are currently active on host server14.</td>
</tr>
<tr>
<td>10410</td>
<td>A new process is listening for incoming TCP connections: Process Name: %1 (PID=%2) Local TCP Port: %3 Local Address: %4</td>
<td>A new process is listening for incoming TCP connections: Process Name: evilagent.exe (PID=20218) Local TCP Port: 2500 Local Address: 192.168.15.56 [myserver.mydomain.local]</td>
</tr>
</tbody>
</table>
A process previously listening for incoming TCP connections is no longer actively listening on this port:

Process Name: evilagent.exe (PID=20218)
Local TCP Port: 2500
Local Address: 192.168.15.56 [myserver.mydomain.local]

5.5.6 Disk Space Monitoring

Monitors disk space usage of fixed drives and issues alerts when limits have been exceeded or trend patterns have changed.

SNMP data is collected by the Heartbeat Agent.

Logical Disks

Monitors either all fixed drives or only selected drives. "Do not monitor any drives" can be used when only Directory Monitoring is required in a package. When monitoring logical drives, volume points that are pointed to by junction points are added to the total / free size calculations when alerts are generated.

Maximum Notification Interval

Only logs a maximum of one event (per disk) in the specified interval while a disk remains in an alerted state (e.g. disk space below an absolute or percentage limit). The maximum notification interval can be configured in the Global Options.

Windows only: If the alert status of a drive toggles between alerted & cleared during the maximum notification interval, such as when disk space constantly increases and decreases right around the configured threshold, then the notification limits below are applied. No more than

- 1 alert per 30 minutes
- 2 alerts per hour
- 3 alerts per every 3 hours
- 4 alerts per every 6 hours
- 5 alerts per every 12 hours
- 6 alerts per every 24 hours

**Limits**
You can either set limits by percentage and/or by a certain size.

![Limits](image)

**Percentage Limits**
To set limits based on the percentage of free disk space, select the option "Alert when percentage of free space is below" and specify a percentage. If this limit is exceeded then EventSentry will log an entry to the Application Event Log with the severity specified in "Log As".

**Dynamic Adjustments:** On larger drives (e.g. > 1Tb), percentage limits often trigger warnings too soon, since 5% of 1Tb still amount to 50Gb. This option uses a proprietary algorithm to adjust the percentage limit dynamically to a more useful threshold. The EventSentry agent will log event ID 10509 (information) describing the calculated limit. This feature supports volumes with a total capacity of ~80Gb or more.

"Dynamic limits are only available on Windows-based hosts."

**Absolute Limits**
To set limits based on the free bytes available on a drive, select the "Alert when free disk space is below" option and specify the number of megabytes or gigabytes. If this limit is exceeded then EventSentry will log an entry to the Application Event Log with the severity specified in "Log As".

Hard limits set to a number higher than the total amount of disk space available on a drive will be ignored. E.g., if the limit is set to alert below 200Gb, but the total size of the drive is only 80Gb, then no alert will be issued.

**Override**
Disk space limits can be overwritten/customized on a per-host basis which avoids having to create multiple disk space packages to support different limits for some hosts. See Override for more details.

**Trend Detection**
Disk space usage is collected over longer periods of time, two days by default. EventSentry can determine whether disk activity is unusually high, even though a percentage or absolute limit have not been exceeded. You can adjust the sensitivity of trend detection by adjusting the percentage.

If a trend change is detected then EventSentry will log an entry to the Application Event Log with the severity specified in "Log As". If you wish to not collect disk space information on weekends then check the "Do not collect trend information on weekends" check box.
Example: If the free disk space decreases by about 100Mb every day, then a decrease of 200Mb would be considered a 100% change.

**Disk Space Data Collection**
Selecting "Record to database" will store historical disk space data in the database and make this data available in the web reports.

<table>
<thead>
<tr>
<th>Database</th>
<th>Primary Database</th>
<th>every 1</th>
<th>hour(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record to database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enumerate 250 largest files</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please note that volumes pointed to by junction points are not taken into consideration when disk space information is recorded in the EventSentry database.

**Enumerate 250 largest files**
When selected, EventSentry will make the 250 largest files on each monitored volume available in the web reports.

**Disable OS disk space monitoring**
Windows automatically writes an entry to the event log when free disk space is below 10%. To avoid duplicate disk space notifications, the built-in alerts by the OS can be disabled by clicking on the "Disable OS disk space monitoring" button.

If you change your mind at a later time then you can activate OS disk monitoring again by clicking on the same button (which will read “Enable OS disk space monitoring”).

5.5.6.1 **Override**

The Diskspace Overrides dialog can be used to customize disk space settings on a per-host basis without having to create and assign multiple disk space packages. Clicking the Override button will bring up the "Diskspace Overrides" dialog where multiple hosts can be added.

To add a host, simply click the + icon and select an existing host from the Hostname drop-down dialog and specify the customized settings. To remove customized settings and revert to the default settings from the package, select the host and click the - button. Clicking Close will store all settings.
### 5.5.6.2 Event Log

The following events are be logged by this feature with the **Disk Space Monitoring** event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| 10500    | Disk space is below a configured percentage limit.          | Free disk space for drive C: (BOOT) is below the configured limit of 15 percent. 12 percent of disk space (756 Mb) are currently available on drive C:.

**Top 5 Directories:**
- 001: [16.84 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL (18084796490 bytes)
- 002: [4.01 GB] C:\System Volume Information (4307181526 bytes)
- 003: [2.71 GB] C:\Windows\winsxs (2909796747 bytes)
- 004: [1.89 GB] C:\Users\bax (2030310546 bytes)
- 005: [1.89 GB] C:\Users\bax\AppData\Local\Microsoft\Windows (2030179456 bytes)

**Top 5 Files:**
- 001: [15.87 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\tempdb.mdf (17043095552 bytes)
- 002: [3.97 GB] C:\System Volume Information\{a9bac31b-02f0-11e7-89ee-0010195ff0e6}\{1843876b-c276-3e48-b7ae-04046e6cc7528} (4261412864 bytes)
- 003: [920 MB] C:\Windows\SoftwareDistribution\DataStore\DataStore.edb (964755456 bytes)
- 004: [800 MB] C:\pagefile.sys (838860800 bytes)
<table>
<thead>
<tr>
<th>Event Number</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10501</td>
<td>Disk space is below a configured absolute limit.</td>
<td>Free disk space for drive C: is below the configured limit of 1024 Mb. 877 Mb of disk space are currently available on drive C:. Top Directories: see 10500 event above. Top Files: see 10500 event above.</td>
</tr>
<tr>
<td>10502</td>
<td>Trend analysis has detected an usually high disk space consumption.</td>
<td>Trend analysis has determined unusual high disk usage on drive D:. The average recorded trend on drive D: was 8976 kb, the current trend was 25432 kb, an increase of 283%. If this trend change is expected (for example, caused by a daily backup routine) then you will see this message two more times before the pattern is recognized. With the recorded trend, disk space will be exhausted in 62 days, with the current trend in 15 days.</td>
</tr>
<tr>
<td>10504</td>
<td>Delayed directory file analysis is complete</td>
<td>Directory and file analysis of drive E: has been initiated by an earlier 10500 or 10501 event and is now complete. Top 5 Directories: 001: [16.84 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL (18084796490 bytes) 002: [4.01 GB] C:\System Volume Information (4307181526 bytes) 003: [2.71 GB] C:\Windows\winsxs (2909796747 bytes) 004: [1.89 GB] C:\Users\bax (2030310546 bytes) 005: [1.89 GB] C:\Users\bax\AppData\Local\Microsoft\Windows (2030179456 bytes) Top 5 Files: 001: [15.87 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\tempdb.mdf (1704309552 bytes) 002: [3.97 GB] C:\System Volume Information{a9bac31b-02fc-11e7-89ee-00101915f0e6}1843876b-c276-3e48-b7ae-04046e6cc752 (4261412864 bytes) 003: [920 MB] C:\Windows\SoftwareDistribution\DataStore\DataStore.edb (964755456 bytes) 004: [800 MB] C:\pagefile.sys (838860800 bytes) 005: [496 MB] C:\Windows\winsxs\ManifestCache\a786a517e28d5687_blobs.bin (520795521 bytes)</td>
</tr>
<tr>
<td>10509</td>
<td>Percent limit has been dynamically adjusted</td>
<td>The percentage-based threshold on drive C: has been dynamically adjusted from 5% percent to 1.58% percent based on the total drive size of 129 GB. A low disk space alert will be</td>
</tr>
</tbody>
</table>
triggered when the available space on this volume falls below 841 MB.

<table>
<thead>
<tr>
<th>Event Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10550</td>
<td>Disk space is back above the percentage limit.</td>
</tr>
<tr>
<td></td>
<td>Free disk space for drive C: (BOOT) is back above the configured limit of 15 percent. 20 percent of disk space (1120 Mb) are currently available on drive C:</td>
</tr>
<tr>
<td>10551</td>
<td>Disk space is back above the absolute limit.</td>
</tr>
<tr>
<td></td>
<td>Free disk space for drive C: (BOOT) is back above the configured limit of 1024 Mb. 1325 Mb of disk space are currently available on drive C:.</td>
</tr>
</tbody>
</table>

### 5.5.7 Directory Monitoring

Directory Monitoring monitors the size or file count of a directory and triggers alerts when the total size (or file count) of a directory is either above or below a set limit. Additional configuration options, such as whether to monitor the physical or the logical size of a directory and whether to include subdirectories are available.

Directory Monitoring is part of the **Disk Space** system health object, and can either be added to an existing system health package that already contains a disk space object, or added to a new system health package / disk space object.

**Adding to an existing object**

To add this feature to an existing system health package, simply select the “Disk Space” object in the system health package and click the **Directory Monitoring** tab.

**Creating a new system health package**
Create a new system health package by right-clicking the "System Health Packages" container and add a new "Disk Space" object to the package by right-clicking the package and selecting "Add". You can also select an existing system health package that already contains a "Disk Space" object and click it in the left pane.

Since the package is only going to be used to monitor directories, set the disk space monitoring feature ("Logical Disks" area) to "Do not monitor any drives" and click the "Directory Monitoring" tab.

**Database**
- Specify the database that will be used when a directory is configured to record the current size to the central database.

**Monitoring a Directory**
- To monitor a new directory, click the + button or double-click an existing directory.

**Directory**
- Select the directory you want to monitor, such as D:\Program Files\Exchange. You can also use environment variables such as %SYSTEMROOT%. Monitoring a UNC path (such as \SERVER1\Payroll) is not supported, you must use the real directory of the network share, such as D:\Payroll.

**General**
- Specify the size or file count limit of the folder. Limits can be specified either in Mb, Gb, Tb. To monitor the file count set this option to "files".

- Also specify whether the size of the folder should be calculated using the physical size or the logical size of the files (this is ignored for file count monitoring). Since hard disk are arranged in sectors, the physical size is usually slightly larger than the logical size, with the exception of folders that have compression enabled. Those directories will usually have a smaller physical size, as such the default and recommended setting is to calculate the physical size.

- Specify how often the agent should check the directory. Since calculating a directory size can be resource intensive on larger directories, set this interval appropriately.

- Check the "Include Sub Folders" check box to include sub directories in the total size calculation.
Actions

Log to Event Log as: Logs an alert to the application event log with the specified severity when the configured threshold is exceeded, see Event Log for more details on events that can be logged by this feature.

Log to Database: Records the current directory size to the database selected in the parent dialog.

5.5.7.1 Event Log

The following events are logged by this feature with the Disk Space Monitoring event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10510</td>
<td>The directory size is above the configured limit.</td>
<td>The physical size of folder &quot;C:\TempStorage&quot; is above the configured limit of 1,048,576 bytes. Folder Information: Logical Size: 41,864,341 Physical Size: 42,192,896 Files: 115</td>
</tr>
<tr>
<td>10511</td>
<td>The directory size is below the configured limit.</td>
<td>The physical size of folder &quot;C:\TempStorage&quot; is below the configured limit of 100,048,576 bytes. Folder Information: Logical Size: 41,864,341 Physical Size: 42,192,896 Files: 129</td>
</tr>
<tr>
<td>10512</td>
<td>The number of files in the folder exceeded the maximum threshold.</td>
<td>The maximum file count of 500 files in folder &quot;C:\MySoftware\Temp&quot; was exceeded, 506 files were found. Folder Information: Logical Size: 41,864,341 Physical Size: 42,192,896 Files: 506</td>
</tr>
<tr>
<td>10513</td>
<td>The number of files in the folder is below the minimum.</td>
<td>Folder &quot;C:\MySoftware\Temp&quot; contains 488 files, which is below the minimum of 500 files. Folder Information: Logical Size: 41,864,341 Physical Size: 42,192,896 Files: 488</td>
</tr>
<tr>
<td>10560</td>
<td>The directory size is back below the configured limit.</td>
<td>The physical size of folder &quot;C:\TempStorage&quot; is back below the configured limit of 1,048,576 bytes. Folder Information: Logical Size: 964,341</td>
</tr>
</tbody>
</table>
### 5.5.8 Software / Hardware Inventory

The software / hardware inventory functionality provides a complete, searchable hardware, software, patch and virtual-machine inventory along with the ability to issue alerts when software is (un)installed, or when applications register themselves in certain registry keys. Combined with Service Monitoring and File Monitoring, EventSentry will detect the majority of changes made to system.
Virtual Machine Inventory (Hyper-V & VMWare)

Inventories all virtual machines from Hyper-V or VMWare hosts as well as the version number of the virtual machine host. Hyper-V inventory is automatically performed when Hyper-V is detected on the host where the EventSentry agent is running. VMWare inventory information is obtained via SNMP when the required SNMP OIDs exist. The following information is available:

**Virtual Machine Host**
- Host Name
- Product Name
- Product Version

**Virtual Machines**
- Host Name
- Status
- CPU Count
- Memory
- Operating System (if available)

VMWare inventory requires that SNMP is enabled on the VMWare ESXi hosts.

Monitor WiFi Connections

Tracks all WiFi activity and shows which Wireless network an adapter is connected to along with a history of all connections and disconnections. The EventSentry agent will also log events to the event log every time an adapter connects or disconnects from a WiFi network, which allows for automation using filters.

The following details are available:
• Adapter Name & GUID
• Status
• Signal Strength
• SSID
• Cipher (e.g. RSNA with PSK)
• Authentication (e.g. CCMP)

Monitoring Batteries & UPS Devices
Monitors built-in batteries in laptops as well as attached UPS devices (if detected by Windows). The current battery status, charge level as well as the total battery capacity are available on the "Host / Inventory" page in the web-based reporting. EventSentry can also shut down a host if the battery status falls below a configurable percent threshold or when the estimated runtime is less than a preset limit, irrespective of the UPS manufacturer and/or model.

Backup MBR and BootLoader and detect changes
Downloads sectors 0-77 as well the sectors 2048-2057 of all hard drives on the monitored system. If changes are detected on the monitored sectors, an event is logged indicating how many bytes were changed and whether the MBR or BootLoader were changed. All monitored sectors are also stored in the database when the agent starts (if enabled) and can be downloaded on the "Host / Inventory" page in the web-based reporting.

This feature is intended to provide some protection against certain Ransomware infections. The events logged when monitored sectors are changed can be used to trigger actions like hibernation, a logoff or a shutdown. The sector backups can be downloaded to a USB boot disk and restored manually in case the original sectors have been overwritten inadvertently.

Software Inventory
If an application is installed an registers itself in the Control Panel under Add/Remove Programs, then EventSentry will notify you and log which application was installed or removed.

If an application does not register itself in Add/Remove Programs, for example if it is installed on a per-user basis, then EventSentry will not detect it. You might still be notified if the application registers itself in one of the many autorun registry keys.

The following information is stored in the database and can be queried using the web reports when the "Record in database" check box is checked:

• Software Name
• Installation Directory*
• Software Publisher*
• Software Version*
• Platform Information (32-bit vs 64-bit)

This feature will also write application history to the database, enabling you to find out when software was installed/uninstalled (note that this information might also be available through the event logs).

Monitoring Web Browser Extensions
Monitor all installed extensions for the following web browsers

• Mozilla Firefox
• Google Chrome
• Microsoft Edge (chromium-based)
and provides a full inventory/history as well alerts when extensions are installed or uninstalled. Browser profiles are supported as well. The following extension information is captured:

- Name
- Publisher
- Version
- Enabled/Disabled
- Publisher (when available)
- Username

Please see below for limitations of this feature since there is no official standard on how browser extensions are stored.

- Under some circumstances the extension name may not be displayed, in which case the publisher is shown instead.
- An extension will show up as **enabled** if it is installed in multiple profiles and enabled in at least one profile.

### Patch Inventory

All installed Microsoft patches are collected and can be queried through the web reports. EventSentry can also issue alerts when a patch is (un)installed. The following information is available:

- Patch Name
- Platform Information (32-bit vs 64-bit)
- Installation Date
- Installation Directory (if applicable)
- Publisher

### Hardware Inventory

The following hardware information is captured; Hardware information is obtained through file information, registry data and WMI:

- Operating System, including Edition and Service Pack
- The location of the SYSTEMROOT directory
- Date when the Operating System was installed
- Whether the machine is running the x64-bit edition of the OS
- Configured UAC level (Vista and later)
- Whether the machine is a Terminal Server, running Hyper-V or Server-Core
- If the machine is a virtual machine, and in some cases the type of VM platform (e.g. VMWare ESX)
- Installed CPUs (including type, speed and number of CPU's installed)**
- The number of installed CPUs, including Hyper-Threading and multi-core detection
- Registered owner and registered company** (if available)
- Computer manufacturer and model** (if available)
- Chassis type (e.g. rack-mount, mini tower, laptop, etc.)
- Warranty information (DELL, HP, IBM & Lenovo hardware only)
- BIOS Version***
- Serial Number, Service Tag (depending on manufacturer)***
- Installed Memory, including the maximum memory, number of memory chips installed and free slots available
- Installed network adapters, including adapter name, link speed, IP address (updated & refreshed periodically) and MAC address
- Installed disk controllers, including adapter name, adapter type (IDE/SCSI) and manufacturer
- Make of installed graphics adapter
- The number of CD-ROM, DVD, Floppy and removable drives
- The current uptime
- The maximum uptime of the host since EventSentry was installed
- Highest supported USB version

Basic system and hardware information can also be obtained via SNMP from a remote SNMP agent by polling SNMP counter values. This includes (when available):

- System Information
- Network Interfaces
- Processor, memory & disk space information
- Uptime information

Extended hardware information is available when SSH credentials are configured:

- Time zone
- USB version
- OS Install Date
- Manufacturer details
- Additional CPU details

The Heartbeat Agent retrieves data from Non-Windows hosts via SNMP and/or SSH.

On DELL© and HP© servers with the appropriate vendor system management tools installed, EventSentry will also collect the following information when installed:

- Status of redundant power supplies (PSUs)
- Current temperature of installed temperature sensors
- Current status and RPM of installed fans
- Availability and IP address of any installed remote management cards
- Status and details of any installed hardware RAID controller (e.g. model number, cache size, firmware version)
- Status of all configured RAIDs (including stripe size (when available), status, raid level)
- Status of all installed physical hard drives, including drive details such as model number, serial number

**HP GEN 10+ SERVERS:** Starting with its generation 10, obtaining managed hardware info from HP servers - with the exception of physical disk (raid) information - requires an iLO card that does not share the same network interface as the Windows OS.

Since iLO cards require authentication, two variables will need to be set on the host(s) or group(s) of servers with Gen 10 iLO cards:

- **HPILOUSER** iLO User
- **HPILOPASS** Password
Upon agent start, the hardware inventory feature can also log an event to the event log if the number of the following installed hardware devices changes since the last time the EventSentry agent was running:

- Installed Memory
- Number of installed processors
- Number of installed floppy drives
- Number of installed CDROM drives
- Number of installed DVD drives
- Number of removable drives
- Link speed of a network adapter
- Addition / Removal of a USB drive
- S.M.A.R.T. status error of a physical drive

Ignore GUID-only applications: Some software will write only the GUID (a hexadecimal number) to the registry when installed. Check this box to ignore software without a useful display name.

System hardware information is updated every time the EventSentry service is started.

Uptime Monitoring
The current uptime of a host is refreshed every 5 minutes and provides the following functionality:

- Keeps track of the maximum uptime across multiple reboots. This can help isolate problematic servers that are rebooted often
• Stores uptime history in the database, which can be accessed through Heartbeat - Availability - Uptime History. The uptime history is updated every time the OS is booting, and records how long the OS was running before the current boot process.

The uptime history keeps track of how long the OS was running between reboots and is only updated when you reboot a host.

Autorun Registry Keys
Some applications register files to automatically run when the computer starts or when a user logs on to the system. While those files are usually required and harmless, this is unfortunately misused by Spyware, Trojan horses and viruses.

EventSentry monitors certain registry locations and will notify you when an application is added or removed from one of the monitored locations. Please note that only HKEY_LOCAL_MACHINE registry keys, which affect all users on the system, are monitored at this time. HKEY_CURRENT_USER keys are not monitored.

EventSentry monitors the following registry values:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Shell

EventSentry monitors the following registry keys:

HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup
HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logon

Autorun Directories
In addition to the registry keys listed above, this feature will also monitor the following directories and notify you if a file is added:

<Documents and Settings>\All Users\Start Menu\Programs\Startup

Additional Information
The Active Setup\Installed Components registry subkey is intended to be used by installations to make sure that all users on a system have up-to-date information in their profile, and as such is examined every time a user logs in. This key has unfortunately been misused by software to install and run malicious applications. We urge you to investigate all changes to this registry key to make sure only authorized applications register themselves there.

Please see the next chapter for all event records logged to the application event log by this feature.

* The amount of information recorded by EventSentry depends on the information provided by the installation routine of the particular software. It is up to the software vendor to determine how much installation they will record in the registry. Most modern software will log the name, publisher and version of the application installed.

** Some information might not be available. Model and manufacturer is only available on most pre-installed computers; registered company is only available if specified during installation; in some cases CPU's information (especially older models) will not show the CPU type.
## 5.5.8.1 Event Log

The following events are be logged by this feature.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Category</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>12000</td>
<td>Software Monitoring</td>
<td>An application was installed.</td>
<td>Application {51A3EF81-FAAF-4E70-815C-74D34D4EC313} (Backdoor Manager) was installed. Additional Information: Publisher: Global Intruder Corp Installation Directory: C:\Program Files\BDM</td>
</tr>
<tr>
<td>12001</td>
<td>Software Monitoring</td>
<td>An application was uninstalled.</td>
<td>Application {51A3EF81-FAAF-4E70-815C-74D34D4EC313} (Backdoor Manager)</td>
</tr>
<tr>
<td>12002</td>
<td>Software Monitoring</td>
<td>An application or file registered itself in a autorun registry key and will be run automatically when a user logs on.</td>
<td>Application badtrojan.exe registered itself in the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Run and will be automatically run when a user logs into the system.</td>
</tr>
<tr>
<td>12003</td>
<td>Software Monitoring</td>
<td>An application or file registered itself in the registry by changing a value.</td>
<td>The registry value Shell in key HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon changed from &quot;explorer.exe&quot; to &quot;badandevilshell.exe&quot;. All files specified in this value will be automatically run when a user logs into the system.</td>
</tr>
<tr>
<td>12004</td>
<td>Software Monitoring</td>
<td>An application was removed from an autorun registry key.</td>
<td>Application desktophog.exe was removed from the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Run and will no longer be run when a user logs into the system.</td>
</tr>
<tr>
<td>12005</td>
<td>Software Monitoring</td>
<td>A file was registered in an autorun directory.</td>
<td>The application eraseallfiles.exe registered itself in the directory c:\Documents and Settings\All Users\Start Menu\Programs\Startup and will be automatically run when a user logs into the system.</td>
</tr>
<tr>
<td>12006</td>
<td>Software Monitoring</td>
<td>A shortcut was registered in an autorun directory.</td>
<td>The shortcut PerformanceEnhancer.lnk (using file c:\windows\evilvirus.exe) registered itself in the directory C:\Documents and Settings\All Users\Start Menu\Programs\Startup and will be automatically run when a user logs into the system.</td>
</tr>
<tr>
<td>12007</td>
<td>Software Monitoring</td>
<td>A shortcut was removed from an autorun directory.</td>
<td>The shortcut PerformanceEnhancer.lnk (using file c:\windows\evilvirus.exe) was removed from directory C:\Documents and</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>12008</td>
<td>Software Monitoring</td>
<td>An application registered itself in an autorun registry key and will be run automatically when the computer starts. Application YourPersonalAdware.exe was added to the registry key HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup and will be automatically run when the system boots.</td>
<td></td>
</tr>
<tr>
<td>12009</td>
<td>Software Monitoring</td>
<td>An application was removed from an autorun key and will no longer be run when the system boots. Application YourPersonalAdware.exe was removed from the registry key HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup and will no longer be run the system boots.</td>
<td></td>
</tr>
<tr>
<td>12010</td>
<td>Software Monitoring</td>
<td>An application registered itself in a registry key and might be automatically run when a user logs into the system. The application SmartTrojan registered file c:\windows\eraseanddestroy.exe in registry key HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components and might be automatically run when a user logs into the system. Please see the help file (search for ACTIVE SETUP) for more information.</td>
<td></td>
</tr>
<tr>
<td>12011</td>
<td>Software Monitoring</td>
<td>An application removed itself from a registry key and will no longer be run when a user logs into the system. Application SmartTrojan (using file c:\windows\eraseanddestroy.exe) was removed from the registry key HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components and will no longer be run when a user logs into the system.</td>
<td></td>
</tr>
<tr>
<td>12012</td>
<td>Software Monitoring</td>
<td>A registry key could not be monitored and the feature disabled itself. There was an error (999) monitoring registry key HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components. Please restart the EventSentry agent or notify NETIKUS.NET support if this problem persists. Autorun monitoring will NOT continue.</td>
<td></td>
</tr>
<tr>
<td>12020</td>
<td>Software Monitoring</td>
<td>A browser extension was installed The %1 browser extension &quot;%2&quot; was added by user %4: Web Browser: %1 Name: %2 Version: %3 User: %4 Enabled: %5</td>
<td></td>
</tr>
<tr>
<td>12021</td>
<td>Software Monitoring</td>
<td>A browser extension was changed / updated The %1 browser extension &quot;%2&quot; was modified by user %4: Web Browser: %1 Name: %2 Version: %3</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Category</td>
<td>Event Description</td>
<td>Field Changed Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1202</td>
<td>Software Monitoring</td>
<td>A browser extension was removed</td>
<td>The %1 browser extension &quot;%2&quot; was removed by user %4:</td>
</tr>
</tbody>
</table>
|      |                   |                                                                                    | Web Browser: %1  
Name: %2  
Version: %3  
User: %4  
Enabled: %5                                                                 |
| 1203 | Hardware Monitoring | The installed memory changed.                                                      | The amount of physically installed memory changed from 512 Mb to 256 Mb.                                                                                  |
| 1203 | Hardware Monitoring | The number of installed processors changed.                                        | The number of installed processors changed from 1 to 2.                                                                                                   |
| 1203 | Hardware Monitoring | The number of installed floppy drives changed.                                     | The number of installed floppy drives changed from 0 to 1.                                                                                                 |
| 1203 | Hardware Monitoring | The number of installed CDROM drives changed.                                       | The number of installed CDROM drives changed from 1 to 0.                                                                                                 |
| 1203 | Hardware Monitoring | The number of installed DVD drives changed.                                        | The number of installed DVD drives changed from 1 to 2.                                                                                                  |
| 1203 | Hardware Monitoring | The number of removable drives changed.                                            | The number of removable drives changed from 0 to 2.                                                                                                      |
| 1203 | Hardware Monitoring | The link speed of a network adapter changed.                                      | The link speed of adapter Gigabit Network Card changed from 1Gb to 100Mb.                                                                                 |
| 1204 | Hardware Monitoring | A removable drive has been added.                                                  |                                                                                                           |
| 1204 | Hardware Monitoring | A removable drive has been removed.                                                |                                                                                                           |
| 1204 | Hardware Monitoring | A drive reported a S.M.A.R.T. status error.                                       |                                                                                                           |
| 1205 | Hardware Inventory | A network adapter connected to a WiFi network.                                   | A network adapter connected to a WiFi network. Connection details:                                                                                         |
|      |                   |                                                                                    | Adapter Name: %1  
Adapter ID: %2  
SSID: %3  
Signal Strength: %4  
Cipher Algorithm: %5  
Authentication Algorithm: %6                                                                 |
| 1205 | Hardware Inventory | A network adapter disconnected from a WiFi network.                              | A network adapter disconnected from a WiFi network. Last connection details:                                                                                |
|      |                   |                                                                                    | Adapter Name: %1  
Adapter ID: %2  
SSID: %3  
Signal Strength: %4                                                                                                                                       |
<table>
<thead>
<tr>
<th>EventCode</th>
<th>Module</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>12500</td>
<td>UPS</td>
<td>Monitoring</td>
<td>At least one battery has been detected and will be monitored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EventSentry will monitor the attached UPS devices and/or built-in batteries. 2 detected device(s):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Battery #1: Current Charge: 98%, Voltage=12V, Status=Online, BatterySize=17930mAh</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Battery #2: Current Charge: 86%, Voltage=11V, Status=Discharging, BatterySize=65430mAh</td>
</tr>
<tr>
<td>12501</td>
<td>UPS</td>
<td>Monitoring</td>
<td>The system is running on battery power.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>At least one connected UPS/battery is now running on battery power. EventSentry will periodically log event 12502 with estimated run times until the UPS is back online. EventSentry will perform a system shutdown when the remaining battery or runtime gets below a configured threshold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Battery #1: Current Charge: 97%, Voltage=12V, Status=Online, BatterySize=17930mAh</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Battery #2: Current Charge: 98%, Voltage=12V, Status=Discharging, BatterySize=65410mAh</td>
</tr>
<tr>
<td>12502</td>
<td>UPS</td>
<td>Monitoring</td>
<td>The system continues to run on battery power.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>At least one connected UPS/battery continues to operate on battery power.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Charge Remaining: 85% Estimated remaining runtime: 23411 seconds</td>
</tr>
<tr>
<td>12503</td>
<td>UPS</td>
<td>Monitoring</td>
<td>The system is no longer running on battery power.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All connected UPS/battery devices are back online.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Battery #1: Current Charge: 98%, Voltage=12V, Status=Online, BatterySize=17930mAh</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Battery #2: Current Charge: 100%, Voltage=12V, Status=Online, BatterySize=65410mAh</td>
</tr>
<tr>
<td>12504</td>
<td>UPS</td>
<td>Monitoring</td>
<td>All attached batteries are fully or almost fully charged.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All connected UPS/battery devices are fully or almost fully charged.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Battery #1: Current Charge: 98%, Voltage=12V, Status=Online, BatterySize=17930mAh</td>
</tr>
<tr>
<td>Event ID</td>
<td>Module</td>
<td>Description</td>
<td>Details/Actions</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12510</td>
<td>UPS Monitoring</td>
<td>A system shutdown will be initiated based on a low battery charge level.</td>
<td>The charge level of all attached UPS devices is at or below the threshold of 50% and a shutdown will now be initiated. Battery #2: Current Charge: 100%, Voltage=12V, Status=Online, BatterySize=65410mAh</td>
</tr>
<tr>
<td>12511</td>
<td>UPS Monitoring</td>
<td>A system shutdown will be initiated based on a low remaining runtime.</td>
<td>The estimated runtime of this system is at or below the threshold of 5 minutes and a shutdown will now be initiated. Battery #1: Current Charge: 47%, Voltage=12V, Status=Online, BatterySize=17930mAh</td>
</tr>
</tbody>
</table>
Performance Monitoring can also obtain data via SNMP from a remote SNMP agent by polling SNMP counter values. The collected data is alerted with and presented in the same way Windows performance data is.

SNMP data is collected by the Heartbeat Agent.

Alerts
Issues event log alerts (which can be forwarded to an action, e.g. email) when a certain performance counter exceeds a configured limit. For example, an alert can be triggered when a process uses more than 70% CPU time for more than 10 minutes.

Alerts are highly configurable and allow you to set how often a performance counter is checked (e.g. every 10 seconds) and how long the counter has to remain above your threshold before an error is logged to the application event log. See Alerts for more information.

Leak Detection
Sometimes applications or drivers can leak resources (e.g. memory, handles) over time, resulting in valuable system resources being over utilized. In severe cases a resource leak can even leak to system instability or a crash. EventSentry can detect some resource leaks with the help of certain performance counters. For example, the following performance counters can be monitored to help detect leaks:

- Process(*)\Working Set
- Process(*)\Handle Count
- Memory\Pool Paged Bytes

Performance Data Collection
Using a database, EventSentry can write performance data to a database which can then be queried through the EventSentry web reports. This allows you to see a history of performance data, (e.g. memory usage, CPU usage, etc.) over a period of time using charts and/or raw data.

Performance tracking also allows you to see a current status of all monitored performance counters at a glance to help you get a quick overview of a server's status. See History & Trending for more information.

EventSentry ships with a variety of built-in performance packages already setup, including the Performance System package. This package contains language-agnostic counters which monitor system metrics such CPU usage and memory utilization. The counters in this package cannot be deleted or changed as this can break functionality in the web reports. Monitoring intervals of those counters can be adapted, and additional counters can be added to the package.
5.5.9.1 Counter Configuration

Performance monitoring supports capturing numerical data from three different types of sources:

- Windows Performance Counters
- SNMP data
- Executables

Windows performance counters and output from executables are monitored by the EventSentry agent running on the monitored machine, whereas SNMP counters are monitored by the Heartbeat Agent.

Frequency Interval (Collect data every ...)

The frequency interval determines how often the performance counter values will be obtained/refreshed from the OS. Use low frequencies (< 5 seconds) for volatile performance counters (such as "Processor(*) % Processor Time", "PhysicalDisk(*)\Avg. Disk Queue Length", ...), or when accurate data is needed. Use larger values for performance counters which change slowly (e.g. "Memory\Available MBytes"). Performance data collection is very efficient, and changing the interval will have little impact on the CPU utilization of the EventSentry agent. Still, it is considered good practice to select intervals based on the performance counter.

For SNMP counters, this value cannot be smaller than the heartbeat polling interval.

Name

A descriptive name of the counter, this name will be visible in alerts and the web reports.

Treat data as floating point values
By default, performance counter values are interpreted as integer values, which is usually the best choice. Activate this option to force the performance counter values to be interpreted as floating point numbers (e.g. for performance counter values returning values smaller than 1).

When both a Windows performance counter and a SNMP counter are available, it is recommended to configure both in the same dialog.

5.5.9.1.1 Windows Counters

**Windows Counter**
This is the name of the actual performance counter, as exposed by the Operating System. You can either

- select a commonly-used counter from the drop-down list
- click the BROWSE button to browse a list of all available counters
- enter the name of a performance counter (e.g. `Process(*)\% Processor Time`) manually
- enter the performance counter IDs (e.g. `238(*)\6`) to support this counter on a Non-English Windows OS as well

With the exception of some core performance counters like CPU and Memory, the IDs of many performance counters are specific to a machine. Performance counter IDs can be looked up in the registry under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\NT\CurrentVersion\Perflib`.

**Instances:** If a performance counter contains the string `(*)` then this counter has instances. EventSentry will monitor all instances of a counter, unless excluded (see below).
Inclusions / Exclusions

If a Windows performance counter supports instances (e.g. Process(*)\% Processor Time) then specific instances (e.g. _Total) can be included or excluded based on the setting of the drop-down. Multiple instances can be separated with a comma, wild cards are supported.

For example, the Process(*)\% Processor Time performance counter also includes the Idle instance which is always near 100% (since it shows the unused CPU time) and the _Total instance which measures the total amount of CPU time from all applications. Data from these instances is not usually relevant, so they can both be excluded by setting the drop-down to “Exclude” and the field to Idle,_Total.

Clicking the “Instances” button will show all current instance of the selected performance counter, and any exclusions specified will be selected. If a specified exclusion is not present in the list of instances, clicking the “OK” button in the “Performance Counter Instances” dialog will reset the exclusions.

Calculate with a secondary counter

Some performance counters provide additional insight when their values are used in combination with another performance counter. You can add, subtract, divide or multiply the obtained values of a performance counter with/by the values by of a “secondary” performance counter.

EventSentry also provides built-in performance counters:

[PhysicalMemory] returns the amount of physical memory installed
[CpuCountLogical] returns the number of all available logical processors available (e.g. cores)
[CpuCountPhysical] returns the number of all available physical processors

Use Multiplier
The calculated result can be multiplied with the specified number.

By default, EventSentry includes a performance counter called "Memory Utilization", which takes advantage of the secondary counter capability. The primary performance counter (Available MBytes) is divided by the physical memory ([PhysicalMemory]) and then multiplied by 100 (example: 1522/4096 * 100 = 37.16%).

Counter Description
Shows the performance counter description, usually provided by the Operating System or software manufacturer providing the performance counter.

5.5.9.1.2 SNMP Counters

SNMP Counter
Specify the OID of a SNMP counter in numerical form, e.g. 1.3.6.1.4.1.2021.11.9.0. Basic arithmetic like addition, subtraction, multiplication and division are supported. SNMP values are polled by the heartbeat agent.

Variables are supported for the SNMP Counter field. For example, if you have some devices supporting only SNMP v1, and some supporting SNMP v2c and higher, then you can still use a single performance counter and just override the default OID on a per-host or per-group level. This is useful for networks running multiple versions of SNMP and OIDs that differ between various SNMP versions.
Calculate the network bandwidth and exclude certain instances

**Inclusions / Exclusions**

If a SNMP counter is organized as a table (aka SEQUENCE), then specific “instances” can be included or excluded if the OID describing the instance names is configured through the **Instances** button. When enabling an instance, the index describing the actual instances is required so that data collected by the instances can be distinguished.

If the instance type is set to **Include** and only one instance is specified, a SNMP-based counter is treated like regular SNMP counter, and the instance name will not be stored in the database.

In the example below, all instances are listed under 1.3.6.1.2.1.31.1.1.1.1, with each row of the table describing a network interface.

When an instance is defined, one or more instances can be excluded, or specific instances can be included.
Calculate with a secondary counter

Some SNMP counters provide additional insight when their values are used in combination with another performance counter. You can add, subtract, divide or multiply the obtained values of a SNMP counter with/by the values by of a "secondary" SNMP counter.

Since SNMP counters do support basic arithmetic, the example above could also be calculated with the use of a secondary counter, by specifying the following in the primary SNMP counter field:

\[
\frac{1.3.6.1.2.1.31.1.1.1.6+1.3.6.1.2.1.31.1.1.1.10}{1.3.6.1.2.1.31.1.1.1.15*1600000000}
\]

Testing

A SNMP counter can be tested by clicking the "Test" button and specifying a SNMP-enabled remote host. If the remote host responds to SNMP GET requests, the current data will be displayed on the bottom of the dialog and updated in regular intervals. If the specified computer is already present in an EventSentry group, then any authentication settings applied to that host will be automatically used when sending the SNMP GET request.

Counter Description

Resolves the specified OID(s) using the MIBs configured on the SNMP Trap Daemon dialog.

SNMP Instances

Enable this option when a SNMP OID returns data in a table, meaning multiple instances for the same counter are provided. This usually applies to performance metrics from hardware components like network cards or CPUs, where multiple instances of the same type of performance source exist. The image below shows an example of SNMP data (current CPU utilization by each core from a VMWare(c) host) returned in a table:
SNMP Index: Since data values returned in a table may be missing context they can be associated with another table that describes those values, as shown in the image below. The table describing the instances can be located anywhere in the SNMP tree as long as the indexes (highlighted in yellow) match.

Virtual Instances
A virtual instance is an additional instance (table row) that is created on the fly, with its value being calculated from the existing SNMP values. The value of the virtual instance can either be the average or sum of all existing values. For example, the \_Total instance, which is normally only available on Windows-based hosts, can be created on VMWare(c) hosts by averaging the current CPU utilization of all cores.

Name: The name of the virtual instance
Calculation Type: Average or sum of all values

5.5.9.1.3 Executables
Output from executables (or scripts) can be used as input for performance monitoring to monitor numerical data not available through a Windows performance counter or SNMP.

Executable
Specify the path to the file from which the output should be interpreted. In its most simple form the executable or script will return a single number, multiple values are supported as instances as well. Floating point numbers are supported when the “Treat data as floating point values” check box is checked.

Embedded scripts can be referenced using the @ symbol.

Output from executables and scripts is only evaluated if the %ERRORLEVEL% returned by the process is 0 (zero). Output is discarded if the executable encountered an error and the resulting %ERRORLEVEL% is 1 or higher.
**Instances**

If the output contains multiple values separated by a common delimiter than the various data values can be processed as instances, similar to instances with Windows Performance Counters. Clicking the **Instances** button will bring up the Instances dialog that allows the configuration of the separator along with the field names. Field names are required in order to distinguish the various data values.

**Dynamic Instances**

Dynamic instances are also supported for when the number and/or names of instances are not known ahead of time, for example when enumerating docker containers. To use dynamic instances:

1. Specify an asterisk (*) for the instance name
2. Make sure the executable returns the instance names in CSV format (regardless of what the separator is set to) as the first line
3. The remaining data is interpreted as if static instances were used

**Important Notes**

Processes launched by the EventSentry agent within the context of performance monitoring cannot run for more than 120 seconds.

Executable-based performance counters that are assigned to Non-Windows hosts will be executed by the EventSentry Heartbeat Monitor service (for each host they are assigned to), where either the $HOSTNAME or $IPADDRESS variable can be passed to the executable. It is not recommended to use embedded scripts for Non-Windows hosts, since the Heartbeat Service may not have access to them.

Since the EventSentry Agent usually runs under a privileged account like the LocalSystem account, it's important to ensure that all scripts that will be utilized by this feature are properly secured by NTFS permissions to prevent non-privileged users from injecting code.

Processes launched by the EventSentry agent within the context of performance monitoring cannot run for more than 120 seconds.

**5.5.9.2 Alerts**

Performance alerts notify you when a specified performance counter exceeds your configured threshold by logging an event to the event log. Instead of immediately triggering alert when a performance value exceeds the threshold, all alerts are associated with a time period over which the current performance...
value is evaluated. An alert will only be logged if the average performance value exceeds the limit during for the configured time period, thus reducing unnecessary alerts.

For example, you can be notified if the % of CPU usage is exceeding 80% over a period of 10 minutes. This means that you will not be notified if the CPU time spikes at 100% for 30 seconds.

Enable Event Log Alert with severity
Alerts are always written to the event log, and event log filters are needed to forward these events (alerts) to an actual notification, such as email. Select a severity with which alerts for this counter should be logged to the event log.

Threshold Setting (Alert if value is ...)
Configures the threshold settings if the counter value is below, exceeds, falls below, is between or is not between a threshold.

Time Interval
The configured time interval determines how long the counter value needs to exceed your threshold before an alert is written to the event log.

Enable repeat alerts
When "Enable repeat alerts at an interval of" is unchecked, an event log alert will be generated whenever the current (or average) value of the monitored counter changes from a non-alerted state to an alerted state and vice versa. This setting is not recommended for volatile performance counters (e.g.
CPU usage), as it can result in a large number of alerts; it is better suited for stable performance counters, such as memory usage, handle count and such.

It's generally recommended to enable this option, so that alerts won't be generated more often than the specified interval.

**Enable Repeat Alerts OFF**

If the time interval is set to 10 minutes and the performance counter exceeds the threshold for 40 minutes, then an alert will only be generated once (after the initial 10 minutes have passed). If the counter however falls back below the threshold however and then jumps back up after some time, then another alert will be generated.

The chart below shows this: EventSentry only logs one alert at 2:30, all the subsequent alerts are considered to be part of the first alert and are thus not generated. The alert is cleared at 3:50.

![Chart showing the behavior of alerts]

Note however that a performance counter value which repeatedly moves from an alerted to a non-alerted state may generate more alerts (and "clear alert") events than desired:

![Chart showing more frequent alerts due to counter oscillation]
Enable Repeat Alerts ON

If you check the **Notify at most every** checkbox however and set a time interval, then you will be notified every time this interval has elapsed if the performance counter continues to be in an alerted state. The alert will only stop when the performance counter is back below the threshold.

The chart below shows the same example as above with Notify at most every set to **1 hour**. Since the monitored value is still in an alerted state, EventSentry will log another error at 3:30 and clear the alarm at 3:50.

![Chart showing a repeat alert example](chart.png)

Embedding Charts (for email alerts)

When checked, EventSentry creates a PNG chart from the data collected during the configured time interval (see above, e.g. 30 minutes), and embeds it as the binary data in the event. The EventSentry agent will then attach the embedded binary data as an image to any emails that include the performance alert. As such, this feature is only useful when performance alerts are matched by at least one filter that emails events. The chart includes an automatically calculated trend line in orange.
Enable Trend Detection (Windows Performance Counters only)

Trend detection suppresses alerts of recurring and expected performance alerts, and works best with percentage-based performance counters like CPU usage. Trend detection keeps track of performance counter value averages, and can suppress alerts when the measured value exceeds the configured hard limit - if the current average matches the historical average.

To consider a performance counter average valid, it has to have been collecting data for at least the set number of "weeks", 2 by default. Once the average is considered valid, it will compare the current counter average with the historical counter average, and suppresses the alert if the current value doesn't deviate more than the configured number of percentage points.

To accomplish this, EventSentry keeps track of the average counter value in 12-minute intervals for every weekday. Counter averages are stored in temp files (%SYSTEMROOT%\EventSentry\temp) with filenames starting with "eventsentry_performance_trend", and remain valid across agent restarts.

Detect Leaks (Windows Performance Counters only)

Some performance counters expose resources usage of a service, process or service. Leak detection attempts to find objects which leak resources, without the need of specifying hard limits. Leak detection works best for performance counters which count resources (e.g. handle count, working set bytes, etc.), and does not work for percentage-based performance counters.

Leak detections can be configured in three ways:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Time period used for analysis</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mild</td>
<td>48 hours</td>
<td>will detect fewer potential leaks, but generate fewer false positives</td>
</tr>
<tr>
<td>Moderate</td>
<td>36 hours</td>
<td>balanced setting between mild and aggressive</td>
</tr>
</tbody>
</table>
Leak detection can be combined with the **numerical comparison of the content filter**, to exclude/include leak alerts below or above a particular value. For example, you can enable leak detection for the handle count of processes, but exclude any alerts for handle counts below 5000.

Some processes may appear to be leaking resources, when that behavior is in fact only temporary (e.g. database servers) to satisfy requests. It is recommended that historical counter information is also **consolidated to a database**, so that long-term patterns of the monitored processes can be observed.

## 5.5.9.3 History & Trending

Collecting performance data in a database allows viewing the current performance status and performance data history through the web reports, using either graphical charts or output in HTML / CSV format.

EventSentry gives you flexibility by allowing you to configure custom database intervals for each counter.

**Record in database every ...**
Checking this box will record performance counter values at the specified interval. The logging interval has to be equal or higher than the polling interval, since the polling interval defines how often the data is actually being retrieved from the OS.

**Keep history**
When checked (default), keeps all historical data for this performance value to support viewing trends in the web reports. When unchecked, only keeps the current data of the performance value. This is useful for performance data where only the current value is relevant and keeping historical data is not useful (e.g. toner level of a printer, battery temperature of a UPS).

EventSentry writes the **average of the data collected over the logging interval to the database**. A shorter logging interval will result in a more accurate representation of the performance data in the database, but will take more more space in the database. For example, if counter data is collected every 5 seconds, and the database logging interval is set to 10 minutes, then EventSentry will calculate the average of 120 collected performance values.
Performance data can be written to one or more databases simultaneously.

### 5.5.9.4 Event Log

The following events are logged by this feature with the **Performance Monitoring** event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Event Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>12100</td>
<td>Performance counter fell below threshold</td>
<td>Alert</td>
<td>The performance counter &quot;%5&quot; (%1) fell below the threshold of %2, the current values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Average: %3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimum: %6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum: %7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Counter Description: %8</td>
</tr>
<tr>
<td>12101</td>
<td>Performance counter (with instance) fell</td>
<td>Alert</td>
<td>The performance counter &quot;%6&quot; (%1&quot;, instance &quot;%2&quot;) fell below the threshold of %3, the current values are:</td>
</tr>
<tr>
<td></td>
<td>below threshold</td>
<td></td>
<td>Average: %4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimum: %7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum: %8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bottom %9 instances: %10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Counter Description: %11</td>
</tr>
<tr>
<td>12102</td>
<td>Performance counter equals value</td>
<td>Alert</td>
<td>The performance counter &quot;%4&quot; (%1) equals the value of %2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Counter Description: %5</td>
</tr>
<tr>
<td>12103</td>
<td>Instance of a performance equals value</td>
<td>Alert</td>
<td>The performance counter &quot;%5&quot; (%1&quot;, instance &quot;%2&quot;) equals the value of %3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Counter Description: %6</td>
</tr>
<tr>
<td>12104</td>
<td>Performance counter exceeds threshold</td>
<td>Alert</td>
<td>The performance counter &quot;%5&quot; (%1) exceeded the threshold of %2, the current values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Average: %3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimum: %6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum: %7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Counter Description: %8</td>
</tr>
<tr>
<td>12105</td>
<td>Instance of performance counter</td>
<td>Alert</td>
<td>The performance counter &quot;%6&quot; (%1&quot;, instance &quot;%2&quot;) exceeded the threshold of %3, the current</td>
</tr>
<tr>
<td>Event Code</td>
<td>Description</td>
<td>Level</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>12107</td>
<td>Counter value is not equal to desired value</td>
<td>Alert</td>
<td></td>
</tr>
<tr>
<td>12108</td>
<td>Counter value (instance) is not equal to desired value</td>
<td>Alert</td>
<td></td>
</tr>
<tr>
<td>12110</td>
<td>Required entry points could not be found in PDH.DLL</td>
<td>Error</td>
<td></td>
</tr>
<tr>
<td>12111</td>
<td>PDH.DLL could not be found</td>
<td>Error</td>
<td></td>
</tr>
<tr>
<td>12114</td>
<td>High handle count due to missing hotfix</td>
<td>Warning</td>
<td></td>
</tr>
</tbody>
</table>

**Event Description:**

- **12107**: The performance counter "%1" (%2) on host %3 does not equal the value of %4, the current value is %5.
  
  **Counter Description:** %6

- **12108**: The performance counter "%1" ("%2", instance "%3") on host %4 does not equal the value of %5, the current value is %6.
  
  **Counter Description:** %7

- **12110**: One or more required function entry points could not be found in the dynamic link library PDH.DLL. Please make sure that the latest version of PDH.DLL is installed on this machine, for example you may copy the DLL from another machine running a later Operating System. Performance monitoring cannot continue.

- **12111**: The dynamic link library PDH.DLL could not be found and is required for performance monitoring. Please make sure that the latest version of PDH.DLL is installed on this machine, for example you may copy the DLL from another machine running a later Operating System. Performance monitoring cannot continue.

- **12114**: The EventSentry agent is experiencing an unusually high handle count (%1 handles) and/or high memory usage (%2 bytes), which is most likely due to a known issue in Windows Server 2003 SP2 (http://support.microsoft.com/kb/938135). It is highly recommended that you navigate to http://support.microsoft.com/kb/938135 to download and install the hotfix to resolve this issue. It is not recommended that you continue to run the agent for an extended time period without installing the Microsoft hotfix. Failure to install the hotfix may eventually result in system instability or a system crash.
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Alert</th>
<th>Details</th>
</tr>
</thead>
</table>
| 12120 | Counter value is between range     | Alert                        | The performance counter "%6" (%1) is between the range of %2 and %3, the current values are:  
|       |                                   |                              | Average: %4  
|       |                                   |                              | Minimum: %7  
|       |                                   |                              | Maximum: %8  
|       |                                   |                              | Counter Description: %8 |
| 12121 | Counter value (instance) is between range | Alert | The performance counter "%7" ("%1", instance "%2") is between the range of %3 and %4, the current values are:  
|       |                                   |                              | Average: %5  
|       |                                   |                              | Minimum: %8  
|       |                                   |                              | Maximum: %9  
|       |                                   |                              | Counter Description: %10 |
| 12122 | Counter value not between range    | Alert                        | The performance counter "%6" (%1) is not between the range of %2 and %3, the current values are:  
|       |                                   |                              | Average: %4  
|       |                                   |                              | Minimum: %7  
|       |                                   |                              | Maximum: %8  
|       |                                   |                              | Counter Description: %9 |
| 12123 | Counter value (instance) not between range | Alert | The performance counter "%7" ("%1", instance "%2") is not between the range of %3 and %4, the current values are:  
|       |                                   |                              | Average: %5  
|       |                                   |                              | Minimum: %8  
|       |                                   |                              | Maximum: %9  
|       |                                   |                              | View recent performance data from web reports:%6  
|       |                                   |                              | Counter Description: %10 |
| 12150 | Performance counter is back above threshold | Alert | The performance counter "%4" (%1) is back above the threshold of %2, the current values are:  
|       |                                   |                              | Average: %3  
|       |                                   |                              | Minimum: %6  
|       |                                   |                              | Maximum: %7  

© <2002 - 2022> ... NETIKUS.NET ltd
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Alert Cleared</th>
<th>Details</th>
</tr>
</thead>
</table>
| 1215 | Instance of a performance counter is back above threshold | Alert Cleared | The performance counter "%5" ("%1", instance "%2") is back above the threshold of %3, the current values are:  
Average: %4  
Minimum: %7  
Maximum: %8  
Counter Description: %9 |
| 1215 | Performance counter is back below threshold | Alert Cleared | The performance counter "%4" (%1) is back below the threshold of %2, the current values are:  
Average: %3  
Minimum: %6  
Maximum: %7  
Counter Description: %8 |
| 1215 | Instance of a performance counter is back below threshold | Alert Cleared | The performance counter "%5" ("%1", instance "%2") is back below or at the threshold of %3, the current values are:  
Average: %4  
Minimum: %7  
Maximum: %8  
Counter Description: %9 |
| 1215 | A previously alerted performance counter is not available anymore | Alert Cleared | The performance counter "Process(*)\% Processor Time" (instance "setup") which previously exceeded the configured threshold, is not available anymore and will not be monitored. |
| 1215 | Performance counter equals value again | | The performance counter "%1" (%2) on host %3 equals the value of %4 again.  
Counter Description: %5 |
| 1215 | Performance counter (instance) equals value again | | The performance counter "%1" ("%2", instance "%3") on host %4 equals the value of %5 again.  
Counter Description: %6 |
| 1217 | Counter value not between range | Alert Cleared | The performance counter "%5" (%1) is not between the range of %2 and %3 anymore, the current values are:  
Average: %4  
Minimum: %6 |
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Alert Status</th>
<th>Detailed Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>12171</td>
<td>Counter value (instance) not between range anymore</td>
<td>Alert cleared</td>
<td>The performance counter &quot;%6&quot; (&quot;%1&quot;, instance &quot;%2&quot;) is not between the range of %3 and %4 anymore, the current values are: Average: %5 Minimum: %7 Maximum: %8 Counter Description: %9</td>
</tr>
<tr>
<td>12172</td>
<td>Counter value back between range</td>
<td>Alert cleared</td>
<td>The performance counter &quot;%5&quot; (%1) is back between the range of %2 and %3, the current values are: Average: %4 Minimum: %6 Maximum: %7 View recent performance data from web reports: %8 Counter Description: %9</td>
</tr>
<tr>
<td>12173</td>
<td>Counter value (instance) back between range</td>
<td>Alert cleared</td>
<td>The performance counter &quot;%6&quot; (&quot;%1&quot;, instance &quot;%2&quot;) is back between the range of %3 and %4, the current values are: Average: %5 Minimum: %7 Maximum: %8 Counter Description: %9</td>
</tr>
<tr>
<td>12174</td>
<td>Counter leak detected</td>
<td>Alert</td>
<td>EventSentry detected a potential leak for performance counter &quot;%1&quot; (&quot;%2&quot;) over the last %3 hours. During this time, the counter value increased from %4 to %5, with an average increase of %6% per hour. Out of a total of %3 hours, the hourly average increased %7 times (%8%). Average: %9 Minimum: %10 Maximum: %11 If available, then you should review the performance data history in the web-based reporting to determine whether you need to take</td>
</tr>
<tr>
<td>ID</td>
<td>Action</td>
<td>Description</td>
<td>Details</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>12175</td>
<td>Counter leak (instance) detected</td>
<td>Alert EventSentry detected a potential leak for performance counter &quot;%1&quot; (%2, instance &quot;%13&quot;) over the last %3 hours. During this time, the counter value increased from %4 to %5, with an average increase of %6% per hour. Out of a total of %3 hours, the hourly average increased %7 times (%8%).</td>
<td>Average: %9 Minimum: %10 Maximum: %11 If available, then you should review the performance data history in the web-based reporting to determine whether you need to take action. If this counter value is not leaking memory, then you may be able to adjust the leak detection settings in the management console.</td>
</tr>
<tr>
<td>12176</td>
<td>Counter leak is resolved</td>
<td>Alert The potential leak for performance counter &quot;%1&quot; (%2) has been resolved, during the last %3 hours the hourly average increased %4 times. The current values are:</td>
<td>Average: %5 Minimum: %6 Maximum: %7</td>
</tr>
<tr>
<td>12177</td>
<td>Counter leak (instance) is resolved</td>
<td>Alert The potential leak for performance counter &quot;%1&quot; (%2, instance &quot;%10&quot;) has been resolved, during the last %3 hours the hourly average increased %4 times. The current values are:</td>
<td>Average: %5 Minimum: %6 Maximum: %7</td>
</tr>
</tbody>
</table>
Binary data of performance alerts (events) which are dispatched to an email action is converted to images which are subsequently attached to the email alerts. It is not shown as binary data. This is because the EventSentry agent, if configured, generates chart images which are then attached to the event as binary data.

5.5.10 File Change & Integrity Monitoring


File change monitoring monitors one or more directories and generates alerts when changes to specified files in a directory occur:

- a file was added to a directory
- a file was removed from a directory
- a file increased in size
- a file decreased in size
- a file changed its checksum (SHA256)

In addition, EventSentry can log all changes to the database and allows viewing of the current status and the history of changes made in the monitored directories. The following file properties are available in the web reports:

- Version
- Hash (SHA256)
- Size
- Entropy
- Digital Signature (when available)
- Stream info
Monitoring Interval / Type

Monitor folder(s) in real time

By default, the listed directories will be monitored in real time. This means that the OS will notify EventSentry when changes in the affected directories occur. This is the most efficient monitoring option, but might add unnecessary overhead if the monitored directory contains a large number of files that change frequently.

When monitoring directories in real time, checking "Only verify checksum when last write time changed" is recommended.

Setting a recurring monitoring option in addition to monitoring folders in real time is also recommended in case the OS does not send real time notifications to EventSentry.

Monitor every X seconds

Instead of monitoring folders in real time, files can also be monitored with a recurring schedule, for example every 10 minutes. This is useful for directories that contain a large number of files that change very frequently, or for directories where real time notifications are not required.

The file monitoring feature can potentially consume a significant amount of CPU time, especially when using the checksum feature and when monitoring folders containing many files.
If folders containing thousands of files need to be monitored, and the CPU time of the EventSentry agent is higher than expected, then please carefully consider and adjust the following settings:

- "Monitor every x minute(s)" should be increased from the default of one hour.
- "Ignore checksums for files larger than" may need to be decreased to reduce the number of times a checksum is created.
- "Detect file checksum changes" should be disabled if it is not needed.

Advanced Settings & Optimizations

It is recommended to set the optimization options in this section to reduce the load the EventSentry agent has on the monitored system(s) when monitoring file checksums.

Ignore checksums for files larger than

If the monitored directories contain large files (e.g. files larger than 50Mb), then calculating the checksum might take many minutes and use up most of the available CPU time on a server. By setting a maximum file size for the checksum feature, you can prevent the service from calculating the checksum of large files.

Only verify incremental checksum (log files)

Only calculates & compares the checksum up to the previously known size when a monitored file increases in size. This is useful for files storing transactions, where existing data may not be modified but new data is being added.

Disable folder redirection on 64-bit systems (Wow64)

When running the EventSentry agent on a 64-bit machine and monitoring folders for which the OS has file redirection for 32-bit processes enabled (e.g. %SYSTEMROOT%\SYSTEM32), then the OS will automatically redirect them to their "Windows on Windows" counterpart. For example, C:\Windows\System32 would be redirected to C:\Windows\SysWOW64. Enabling this option will disable folder redirection on 64-bit systems.

Only verify checksum when last write time changed

By default, EventSentry will calculate the checksum of every included file in a monitored directory when a file change is reported by the OS. This, again, can consume a large amount of CPU time if the monitored directory contains a large number of files. By activating this option, the agent will only calculate and compare the checksum of a file if the last write time has changed.

Only verify checksum when file size has changed

By default, EventSentry will calculate the checksum of every included file in a monitored directory when a file change is reported by the OS. This, again, can consume a large amount of CPU time if the monitored directory contains a large number of files. By activating this option, the agent will only calculate and compare the checksum of a file if the file size has changed.

Known Limitations

- It is not recommended to also specify directories which are sub directories of already configured directories when the "Include Sub Directories" option is selected. For example, monitoring both C:\Documents as well as C:\Documents\Finance is not recommended.
- Monitoring UNC paths (e.g. \SERVER1\Payroll) is not supported.

Database

Specify the database that will be used when a directory is configured to record changes to the central database.
5.5.10.1 Managing Directories

To add a directory, click the + icon in the "File Monitoring" section which will bring up the "Add / Edit Monitored Folder" dialog. This dialog lets you specify:

- Which directory to monitor
- Which files to monitor inside the directory
- Which attributes/properties to monitor
- Whether you would like to generate event log alerts upon changes
- Whether to record changes in the database

The directory specified in the Folder field will be monitored, the Browse button can be used to browse to a local folder; environment variables such as %SYSTEMROOT% are supported. Specifying a UNC path such as \Server1\Folder1 is NOT SUPPORTED, you must use the real directory of the network share, such as C:\Payroll. The "Include Sub Directories" option enables monitoring of files and folder in sub directories of the specified directory.
Files
By default, the agent will monitor all files in the specified directory, but you can customize how files are monitored in the specified directory. You can either monitor all files and exclude a subset of files, or only monitor a certain set of files based on extension, file name or sub folder.

Entries in the file list can also be excluded by preceding them with the exclamation mark !. For example, the following configuration will monitor all .exe and .sys files along with the hosts & lmhosts file in the %SYSTEMROOT%\system32 directory but exclude all files in the %SYSTEMROOT%\system32\drivers\wd directory.

Include all files in the selected folder, except for exclusion below
This setting will monitor all files in the selected folder, with the exception of files and/or wildcards listed in the "Exclusions" list. As such, click the + and - icons to add and remove files or patterns that should be excluded from monitoring.

Only monitor files that are included below
Only monitors a particular set of files in the specified directory. Click + and - icons to add and remove files or patterns that should be monitored. For example, to monitor all executable files in a directory, click the + icon and enter *.exe.

Monitor the following changes
- **Detect File Additions**: Detects when new files are added to the directory
- **Detect File Deletions**: Detects when files are deleted from the directory
- **Detect File Checksum Changes**: Detects when the checksum of a file changes, using a 256-bit SHA checksum
- **Detect File Size Increases**: Detects when the size of a file increased
- **Detect File Size Decreases**: Detects when the size of a file decreased

Alerts
You can have the agent log an event to the application event log when a change has been detected, and you can track all changes in a selected database.
Log to Event Log as: Logs changes to the application event log with the specified severity, see Event Log for more details on events that can be logged by this feature.

Log as INFORMATION event if digital signature is valid: EventSentry can verify the digital signature of files and adjust the event severity automatically if a file has a valid signature. This can reduce the noise from file monitoring events by automatically suppressing events from files that are deemed legitimate.

Log to Database: Records changes to the database selected in the parent dialog.

Include file entropy: Enabling this option will calculate and store the entropy of each file in the database.

5.5.10.2 Event Log

The following events are logged by this feature with the File Monitoring event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| 12200    | A SHA-256 checksum change has been detected. | A SHA-256 checksum change has been detected:  
Package: File Integrity System32 x64  
File: C:\WINDOWS\system32\ntoskrnl.exe  
Old Checksum: B2728620F63488A32597DD97EA40F54460C55D97942748716051F60199C682F8  
New Checksum: FE12E1FAEAEE5DDF34A93128C709B69EE88249E6B28B3D279F2E37ADD3EDC52  
Signed: Yes: SHA1 by NETIKUS.NET ltd on 6/15/2018 3:35:51 AM (COMODO RSA Code Signing CA)  
Entropy: 6.53  
The content of the above file has been modified. |
| 12201    | A file size change has been detected. | A file size change has been detected:  
File: C:\WINDOWS\system32\MRT.exe  
Old Size: 12,619,736 byte(s)  
New Size: 13,511,640 byte(s)  
Change: +891,904 byte(s) |
| 12202    | A file has been added. | A file has been added to a monitored directory:  
Directory: C:\WINDOWS\system32  
File: C:\WINDOWS\system32\_000007_.tmp.dll  
Size: 14,640 byte(s)  
Checksum: 93BB82EB2786708ADD9F1538283658EE949AA79E58196F0386AD88FB61320B1  
Signed: no  
Entropy: 7.23  
Version: 3.12.00 |
| 12203    | A file has been deleted. | A file has been removed from a monitored directory:  
Directory: C:\WINDOWS\system32 |
File: _003244_.tmp.dll
Last size: 822,272 byte(s)
Last checksum: FE2FE85EC553E8DFE0B04900EFE5BDA53F0F087730BDEBB95F681A0DF9900938
Last version: 3.12.00

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>122</td>
<td>A directory could not be monitored due to an error. EventSentry was unable to monitor the directory C:\Files for changes due to the following error: Access Denied. The directory will not be monitored.</td>
</tr>
<tr>
<td>122</td>
<td>A directory could not be monitored in real-time due to an error. EventSentry was unable to associate the directory C:\Files with an existing I/O completion port due to error: Access Denied. The directory will not be monitored.</td>
</tr>
<tr>
<td>122</td>
<td>A directory could not be opened / accessed due to an error. EventSentry was unable to open the directory C:\Files due to error: Access Denied. The directory will not be monitored.</td>
</tr>
<tr>
<td>122</td>
<td>A temporary file was upgraded from an earlier, deprecated version of EventSentry.</td>
</tr>
<tr>
<td>122</td>
<td>Indexing of all monitored directories started. File monitoring will now index all monitored directories. This process can take several minutes, depending on the number of files and the performance of the computer. When complete, event 12216 will be logged.</td>
</tr>
<tr>
<td>122</td>
<td>Indexing of all monitored directories is complete. File monitoring has finished indexing all monitored directories.</td>
</tr>
</tbody>
</table>

### 5.5.11 NTP Monitoring

NTP monitoring verifies and optionally corrects the local system time with a RFC 1769 and RFC 1305 NTP server (up to version 3) on the local network and/or the Internet. Network latency is taken into consideration when calculating the clock offset, with a precision down to milliseconds.
Interval (Verify Time)
Specifies how often the local time is compared with the time of the configured NTP server(s).

Maximum Tolerance
The maximum time differences (in ms) that is acceptable between the local host and the NTP server. If the time difference between the local host and the NTP server exceeds the maximum tolerance, then an event is logged to the event log (with the severity specified in Log To Event Log) and the local time is adjusted if configured.

Set Local Time if Outside Tolerance
If the time difference between the local host and the NTP server exceeds the maximum tolerance, then the local time is adjusted to match that of the NTP server.

NTP Servers
The list of NTP servers that are queried in the specified interval. You can specify multiple NTP servers, and servers are processed from the top to the bottom. If a server is unreachable, then the next NTP will be contacted.

Recurring Logging
Check the Log time difference every check box to log an informational event to the event log at the specified interval. The event contains the current time difference between the local host and the NTP server.

Recurring Logging
Check the Log time difference every check box to log an informational event to the event log at the specified interval. The event contains the current time difference between the local host and the NTP server.

5.5.11.1 Event Log
The following events are logged by this feature with the NTP Monitoring event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>12300</td>
<td>A time difference has been detected.</td>
<td>The time difference between this computer and the NTP server &quot;%1&quot; has exceeded the maximum</td>
</tr>
<tr>
<td>Event Code</td>
<td>Description</td>
<td>Message</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12301</td>
<td>A time difference has been detected and the local time has been adjusted.</td>
<td>The local time has been successfully adjusted to %1 after a time difference (%2) has been detected between this computer and NTP server &quot;%3&quot;.</td>
</tr>
<tr>
<td>12302</td>
<td>The local time could not be adjusted due to an error.</td>
<td>The local time could not be adjusted, even though a time difference (%1) has been detected. The error was: %2.</td>
</tr>
<tr>
<td>12303</td>
<td>The current time could not be retrieved from a NTP server.</td>
<td>EventSentry was unable to retrieve the current time from host %1 due to the following error: %2.</td>
</tr>
<tr>
<td>12304</td>
<td>The connection to a NTP host timed out.</td>
<td>EventSentry was unable to retrieve the current time from host %1, the connection timed out.</td>
</tr>
<tr>
<td>12305</td>
<td>EventSentry has been unable to connect to a NTP server for an extended time period.</td>
<td>EventSentry was unable to retrieve the current time from host %1 for %2 seconds. EventSentry will not attempt to connect to this host again for %2 seconds and will try to use the other NTP servers in the list (if available).</td>
</tr>
<tr>
<td>12306</td>
<td>None of the configured NTP servers could be reached.</td>
<td>EventSentry was unable to connect to any of the configured NTP servers (%1). Please make sure that at least one of the listed hosts is a valid NTP server.</td>
</tr>
<tr>
<td>12307</td>
<td>This events logs the current time difference between the local host and the NTP server.</td>
<td>Time difference between local host and %1: %2.</td>
</tr>
</tbody>
</table>

### 5.5.12 Scheduled Tasks

Monitoring scheduled tasks offers inventory and change detection of Windows scheduled tasks.

**Inventory**

The scheduled tasks inventory is accessed through the “Status” menu in the web reports, and includes the following task properties:

- State
- Task Name
- Last Run Result
- Last Run Time
- Number of Actions
- Action Details
- Number of Triggers
- Trigger Details

**History & Change Detection**

Detected changes are either viewed through the “History” menu in the web reports or in the respective event log. Generated events from scheduled task changes can trigger actions such as email alerts. The following changes are detected:

- A scheduled task is added
- A scheduled task is removed
- The actions associated with a scheduled task are changed
- The triggers associated with a scheduled task are changed
- Changes to "Enabled" state
- The user the task runs under is changed

**Refresh Interval**
Configures how often the scheduled tasks on the system are enumerated.

**Event Severities**
Configures the event severity with which a new or removed tasks or changed tasks are logged to the event log.

**Filter Settings**
Specific tasks can be excluded from monitoring ("Exclude tasks listed below"), or only specific tasks can be monitored ("Monitor only tasks listed below") by adding them to the list with the + and - buttons. The "Monitor all tasks" option will clear any filters and monitor all tasks.

- **Ignore Last Result changes**: When the last result of a task changes, do not trigger a change event.
- **Ignore Time Trigger changes**: When the time of a trigger changes, do not trigger a change event.

### 5.5.12.1 Event Log
The following events are logged by this feature with the **Scheduled Tasks** event category.
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>12400</td>
<td>The Scheduled Tasks monitoring engine has been initialized. %1 cached tasks have been found, %2 tasks are currently configured on this system.</td>
<td>The Scheduled Tasks monitoring engine has been initialized. 152 cached tasks have been found, 153 tasks are currently configured on this system.</td>
</tr>
<tr>
<td>12410</td>
<td>A new scheduled task has been added:</td>
<td>A new scheduled task has been added:</td>
</tr>
</tbody>
</table>
|          | Name: %1  
Enabled: %2  
User: %3  
State: %4  
Triggers: %5  
Actions: %6 | Name: Test  
Enabled: 1  
User: DOMAIN\UserA  
State: Ready  
Triggers: Type: Schedule (Daily)  
Enabled: Yes  
Day Interval: 1  
Actions: Type: Start a program  
Path: C:\doit.exe |
| 12411    | A scheduled task has been removed:                                                | A scheduled task has been removed:                                                                                                                                                               |
|          | Name: %1  
Enabled: %2  
User: %3  
State: %4  
Triggers: %5  
Actions: %6 | Name: Test  
Enabled: 1  
User: DOMAIN\UserA  
State: Ready  
Triggers: Type: Schedule (Daily)  
Enabled: Yes  
Day Interval: 1  
Actions: Type: Start a program  
Path: C:\doit.exe |
| 12412    | A scheduled task has been changed:                                               | A scheduled task has been changed:                                                                                                                                                               |
|          | Name: %1  
Field Changed: %2  
New Value: %3  
Old Value: %4 | Name: Microsoft\Windows\WindowsUpdate\AUScheduledInstall  
Field Changed: Triggers  
New Value:  
Old Value:  
Type: Schedule (One time)  
Enabled: Yes  
Time: 2014-11-25T13:00:00Z |
5.5.13 System Status Tray Application

The System Status is an application that, when enabled, is visible in the system tray. Through the tray application the end user can see a quick overview of the current system status, send notes to the web reports (including a screen shot) and utilize a HTTP-based web API to create a support ticket with compatible web sites. The system status application is also referred to as “EventSentry” and is an enhanced version of “EventSentray” that is part of the free EventSentry Sysadmin Tools.

Tray Icon
The tray icon is dynamic and will show an EventSentry logo (with a status overlay) by default. Hovering over the icon will show the current host name along with the current uptime. The app monitors the CPU and disk queue length in the background and will dynamically change the tray icon to either a CPU or DISK icon if high utilization is detected:

- The EventSentry service is running. If the agent is utilizing a remote collector, also confirms that the agent is currently connected to the collector.
- The EventSentry service is stopped.
- The EventSentry service is running but not connected to a collector (only shown if agent is configured to use a collector).
- CPU Alert: CPU usage 85% or higher
- CPU Warning: CPU usage 70% or higher
- Disk Warning: Disk queue length 3 or higher

System Information
The system information dialog shows additional performance stats and system information and can be displayed by either double-clicking the tray icon or by right-clicking the icon and selecting “System Information”.

© <2002 - 2022> ... NETIKUS.NET ltd
The system information dialog and tray icon show the following information:

- Hostname
- Uptime
- EventSentry status
- CPU utilization
- Memory utilization
- Disk utilization
- Disk space usage of all physical disks
- Top 3 processes (CPU utilization)
- Top 3 processes (memory utilization)
- Current IP address and link speed
- Indication whether host needs a reboot
- Battery health (when applicable)
- Other logged on users (if any)

Since the EventSentry application does not run elevated, the top processes shown may not include system processes or processes from other users that are not accessible with the default process elevation level.

Notes

The web reports support adding notes for documentation purposes through the web interface; notes can be tagged with host names to link notes to specific hosts. The tray application supports adding notes without visiting the web interface and also supports attaching screen shots automatically. This makes it extremely easy to document changes & activity that may be useful to other team members.
Support Tickets
When a ticketing system accepts incoming emails and/or provides a web API, the tray application can be configured to allow any logged on user to open support requests. This makes it extremely easy for end users to submit a ticket when they are experiencing an issue. The message submitted will include various stats about the host the ticket was submitted from, including:

- Host name
- Logged-On User
- System stats including OS, uptime, IP address and EventSentry agent version (identical to email footers)

Help Menu
The help menu provides a link to the web-based documentation of EventSentry, and the “Support Package” option creates an archive that contains information that may be relevant for troubleshooting technical issues with the EventSentry agent and includes:

Including screenshots requires that the selected action utilizes the collector and that the collector service runs on the same host as the web reports.
• Debug logs
• configuration
• crash dumps (if any)

The resulting zip file can be uploaded to the support portal.

5.5.13.1 Configuration

The tray application configuration is part of a system health package, just like other system health features.

The settings controls the following features of the tray application:

• Ability to submit notes
• Support for screen shots for notes or support tickets
• Ability to open support tickets

At a minimum, with all options disabled, the tray application will support the system information dialog and the help menu.

Notes
When enabled, adds the "Add Note" menu entry to the tray application which allows users to add notes.

Allow Screenshots
When enabled, allows users to attach screenshots to both notes and support tickets.

![Caution] Including screenshots requires that the selected database utilizes the collector and that the collector service runs on the same host as the web reports.

Support Tickets (requires collector)
This feature utilizes the HTTP action to submit support tickets on behalf of the user, and as such any ticketing system that provides a HTTP API can be integrated.

Custom Menu Entry: Changes the default menu entry “Support Request” to a user-provided entry.
Require Email: Requires the user to provide an email address
Require Subject: Requires the user to specify a subject for the support request

Action: The HTTP action to trigger, must be configured for collector. Data entered by the user is available via the following variables:

   Email: $SUPPORTEMAIL
   Subject: $SUPPORTSUBJECT
   Ticket Details: $MESSAGE
Screenshots are supported for HTTP actions configured for "Form Submission" and can be configured in the "Form field name for attachments" field.

5.6 Security & Compliance

The Security & Compliance features intercept mostly security-related information from the Security event log, normalize the data and collect it in the EventSentry database. These feature are not only useful when you need to comply with federal regulations, but also for general troubleshooting, statistics and easier access to a wealth of security-related data.

See Resources - Compliance - Regulations for additional information on government compliance.

Overview
The following security & compliance features are supported and can be added to a package:

- Process Tracking
- Logon Tracking
- Print Tracking
- File Access Tracking
- Account Management Tracking
- Policy Change Tracking
- Registry Tracking

Adding/Removing objects to/from a Security & Compliance Package
To add a new object to a package, right-click the package and select the desired security & compliance object from the Add submenu:
The new object will appear under the package with a blue wheel icon associated with it. Please note that you cannot add more than one object of the same type to the same package. For example, you cannot add two Registry Tracking objects to the same package.

To remove a security & compliance object, right-click the object and select Remove this object.

5.6.1 Package Options

The package options supports enabling or disabling a package, entering a description, assigning the package or specify a database action on the package level (instead of configuring it in every object).

See "Package Options" for more details.

5.6.2 Requirements

All Security & Compliance features work by intercepting Audit Failure and Audit Success events from the Security events. As such, the respective audit features need to be enabled in the security policy of the computers being monitored. For example, in order to track the creation of new user accounts, the Account Management policy needs to be enabled.

All features can be configured to automatically turn on auditing for you if it's not already enabled, however we still recommend to enable auditing on the domain level using group policies when possible.

Please see the list below to identify which auditing options are required by the respective features:

**Required Audit Configuration for Security & Compliance**

<table>
<thead>
<tr>
<th>Security &amp; Compliance Feature</th>
<th>Windows Auditing Category</th>
<th>Windows Auditing Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Tracking</td>
<td>Windows 2003 and earlier</td>
<td>Windows Vista and later</td>
</tr>
<tr>
<td></td>
<td>Audit process tracking</td>
<td>Detailed Tracking:</td>
</tr>
<tr>
<td></td>
<td>(Success)</td>
<td>- Audit Process Creation</td>
</tr>
<tr>
<td>Logon Tracking (Console</td>
<td>Audit logon events</td>
<td>- Audit Process Termination</td>
</tr>
<tr>
<td>Sessions)</td>
<td></td>
<td>Logon and Logoff:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Logon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Logoff</td>
</tr>
</tbody>
</table>
Once the required auditing options have been determined, one of the following three options can be used to enable auditing. The required auditing setting from the Required Auditing column will be referred to as [Auditing Option].

1. You can have the EventSentry agent automatically enable the required auditing setting when the service starts by selecting "Auditing On" from the Requested Audit Policy. In this case make sure that no top-level policies are overwriting policy settings set by the EventSentry agent.

2. There are multiple ways to enable "Audit process tracking" outside of EventSentry:

   **Windows 2003 without Active Directory**
   Open “Local Security Policy” in the “Administrative Tools”. Navigate to “Security Settings” -> “Local Policies” -> “Audit Policy”. Double-click [Auditing Option] and check the “Success” check box. This change might take several minutes until it becomes effective.

   **Windows 2003 with Active Directory**
   Open the appropriate group policy or open the “Domain Security Policy”. There, navigate to “Audit Policy” and set [Auditing Option] to “Success”. Depending on your Active Directory setup you might need to edit a group policy other than the Domain Security Policy.
Windows 2008 (and higher) with "Force audity policy subcategory settings" enabled

Open the appropriate group policy or open the "Domain Security Policy". There, navigate to "Advanced Audit Policy Configuration" and expand the appropriate category (see table "Required Audit Configuration for Security & Compliance" above). There, configure the required settings to "Audit Success".

3. The security event log "Log Size" needs to be configured to "Overwrite events as needed", it also recommended to specify a size of at least 2048kb. The EventSentry agent will write an error message upon startup to the application event log if the event log is not correctly configured.

You can change the "Log size" settings by opening up "Event Viewer" (from Administrative Tools) and right-clicking "Security Log". Select "Properties" from the menu and verify that the "Log size" is correctly set to "Overwrite events as needed". Also verify that the "Maximum log size" is sufficiently big.

To disable previously enabled Process Tracking of the Operating System, set the Requested Audit Policy to Auditing Off. Make sure that no domain policies undo any policy changes performed by the EventSentry agent.

5.6.3 Process Tracking

Process Tracking will record all process activity (process creation, process exit) in a central database and is intended to monitor application usage on servers and workstations. The collected information can be queried through the web interface to obtain tracking data, history, statistics etc..

Combined with Sysmon and NetFlow, the process tracking feature can provide powerful insights into process activity, including associated network activity, on monitored systems.

Requirements

This feature works by intercepting Audit Success events that are written to the security event log when Audit Process Tracking is enabled in the Local Security Policy of the monitored host. As such, some requirements need to be met before process tracking can function properly. Please see requirements for details.
Configuration

Tracking All Processes (with exceptions)
Select "Track all processes except those listed below" to monitor all processes. To exclude processes click the + button and specify the process executable to exclude (see info box below).

Tracking only selected Processes
Select "Only track processes listed below" and click the + button to add processes that should be monitored to the list.

Processes need to be added either with a wildcard (e.g. *\postgres.exe) or by using the full path (e.g. C:\Program Files (x86)\EventSentry\postgresql\bin\postgres.exe).

Include command line
Captures the command line of processes when enabled. The process command line is either parsed from event 4688 if configured in the OS and present (search for "Process Command Line" here for more details) or queried from the running process. The latter will only work if the process is still running when the agent attempts to obtain this information, and may not work for processes that are only active for a very short amount of time (e.g. less than 1 second).

Performance Warning: If the process command line is not available in event 4688 then EventSentry may utilize WMI to obtain the process command line. This may incur a significant performance penalty, especially on systems with a high process activity.

Security Warning: Use this option with care, command line arguments may include sensitive information such as usernames and passwords.

Sysmon network events
EventSentry can be integrated with the Sysmon v7.x utility from Windows Sysinternals.

Checksum
When enabled, calculates the specified type of checksum (SHA 256, 384 or 512) of every executed process and makes that available in the reporting. Checksums can be correlated with sites like virustotal.com.

It's recommended to enable optimization to reduce the potential CPU load the EventSentry agent has on the monitored system, disable the optimization in high security environments. When optimization is enabled, the agent will temporarily cache the checksum of frequently executed processes. Standard optimization will access cached checksums if the file write time has not changed since the last time a checksum was generated; high optimization will access cached checksums if the same file was executed within the last 5 seconds and if the write time has not changed.

Enabling Process Tracking in the OS
Since process tracking needs to be enabled in the Operating System you can configure the agent to active it automatically if it isn't already activated. Please see requirements for more information.

Database
Select the database action which points to the correct database.

Additional Features
If the specified database is temporarily unavailable, then EventSentry will cache the pending process tracking data and run the transactions when the database server becomes available again.
5.6.3.1 Sysmon Integration

The System Monitor service & driver (Sysmon in short) logs a variety of events - mostly in response to process activity that occurs on a system - to the Microsoft-Windows-Sysmon/Operational event log. Sysmon events are similar to the 4688 and 4689 events logged by Windows to the security event log when a process starts and exits, the events generated by Sysmon are significantly more detailed however and cover other areas such as network activity, file write activity and more.

When configured to log network activity, Sysmon will log an event whenever a Windows process creates a network connection:

![Sysmon logs network activity by slack.exe](image)

When enabled, EventSentry intercepts event id 3 from the Microsoft-Windows-Sysmon/Operational event log which indicates that a local process created a network connection. This data is correlated to process tracking data collected from the Windows security event log and available in the web reports. If Sysmon data is available for a process tracking entry, then a black plus icon will be shown next to the PID in the web reports.

If EventSentry is configured to also collect NetFlow data, the data provided by Sysmon can be used to examine the associated network traffic generated by the process. Every row in the Sysmon report provides a link to the NetFlow History report.
Sysmon Installation
Sysmon can be downloaded from https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#configuration-files and installed from the command line with the following command:

Sysmon64.exe -accepteula -i -n

The -n switch is important as it instructs Sysmon to log network activity from processes. Substitute "Sysmon64.exe" with "Sysmon.exe" on 32-bit systems. Despite of what is stated in the official documentation, a reboot is often necessary to activate the logging of event id 3.

To verify that Sysmon was installed and configured correctly, run `sysmon64 -c` which should yield output similar to what is shown below:

System Monitor v7.03 - System activity monitor
Copyright (C) 2014-2018 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
- Service name: Sysmon64
- Driver name: SysmonDrv
- HashingAlgorithms: SHA1
- **Network connection: enabled**
- Image loading: disabled
- CRL checking: disabled
- Process Access: disabled

It is important that **Network connection** is set to **enabled**.
5.6.4 Logon Tracking

Logon Tracking tracks both successful console logons as well as a variety of network logons - both failed and successful.

Console Logons
Tracks interactive logon sessions made either physically or through remote desktop (terminal services). This feature collects a variety of information about a logon session, such as the source computer, logon durations and more. Please see Console Session for more information.

Network Logons
Network logon tracking includes the following:

- Logon Failure Analysis: Tracks all authentication failures
- Domain Account Authentication: Tracks all successful domain account authentications
- User Logon by Server Type: Tracks all logons

See Network Logons for more information.
5.6.4.1 Console Logons

**Console Logon Tracking** will record all logon activity (interactive logon's and terminal services logon's) in a central database and is intended to monitor logon usage on workstations and servers. The collected information can be queried through the web reports to obtain information such as:

- Which user logged on to which computer
- How long the user was logged on
- Accumulative information such as how long a user was logged on over the course of a time period

**Requirements**

This feature works by intercepting Audit Success events that are written to the security event log when Audit Logon Events is enabled in the Local Security Policy of the monitored host. As such, some requirements need to be met before logon tracking can function properly. Please see Requirements for details.

Windows records logon and logoff activity only on the host where the user is actually logging in. If you intend to monitor logon's and logoff's of all users in a domain environment, then you will have to install the EventSentry agent on all computers where users can log on, including all workstations. You will not be able to track all logon and logoff activity just by installing the EventSentry on the domain controller(s). This is not a limitation of EventSentry, but of Windows itself.

**Collected Data**

EventSentry will collect the following logon information on all supported Windows platforms:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Type</td>
<td>“Console” or “Terminal Services”</td>
</tr>
<tr>
<td>Logon ID</td>
<td>A unique hexadecimal number identifying the logon on the machine</td>
</tr>
<tr>
<td>Computer</td>
<td>The computer where the user logged on</td>
</tr>
<tr>
<td>Group</td>
<td>The group the computer is a member of</td>
</tr>
<tr>
<td>Username</td>
<td>Username of user who logged on/off</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain (or computer name) of user who logged on/off</td>
</tr>
<tr>
<td>Logon Privileges</td>
<td>Whether user is local administrator</td>
</tr>
<tr>
<td>Login Date / Time</td>
<td>Date and time when the user logged on</td>
</tr>
</tbody>
</table>
Monitoring with EventSentry

Logoff Date / Time
Date and time when the user logged off

Duration
The amount of time the user was logged on

Privacy
Since collecting logon information does track a user's activity to some extent, you will still need to make sure that collecting this information does not interfere or violate any corporate policies or laws in place.

Configuration
Tracking All Users (with exceptions)
Select "Track all users except those listed below" to monitor all logon's. To exclude users click the + button and specify the username or part of the username to exclude.

Tracking only selected Users
Select "Only track users listed below" and click the + button to add users that should be tracked to the list.

Track only administrative user logons
When checked, only tracks a console logon if the user logging on is part of the local "Administrators" group - either directly or through nested group membership.

Enabling Logon Tracking in the OS
Since logon tracking needs to be enabled in the Operating System you can configure the agent to activate it automatically if it isn't already activated. Please see requirements for more information.

Database
Select a database action where the logon data should be stored.

RDP Gateway Servers
When utilizing RDP gateway servers, EventSentry can report the actual remote IP address of the client connecting through the gateway server. Resolving IP addresses requires the following:

1. The "Microsoft-Windows-TerminalServices-Gateway" event log is monitored on the RDP gateway server and events are written to the same, collector-enabled database that console tracking is using.
2. The collector is enabled

If the above prerequisites are met then the "Remote IP" address column in the Console report should show the actual IP address of the remote client initiating the RDP connection, and not the IP address of the RDP gateway server.

5.6.4.2 Logon Activity
Network logon tracking collects a wide variety of information about successful and failed logins on a network. Network logon tracking is useful in a variety of scenarios:

- Regulatory Compliance
- Network Security Review
- Troubleshooting
- Network Logon Statistics

For example, the following statistics / reports can be created with the data gathered:

- Most common reasons for failed logons
- Servers / Workstations with most failed logons
- Most common logon types (e.g. service, interactive, etc.)
- Protocol distribution (e.g. NTLM vs. Kerberos)
and much more

Logon Failures
Documents all authentications to domain controllers by users. Note that whenever such a user logs onto their own workstation or member server, this will generate a Network logon to a DC since the user’s workstation must access the domain controller under the user’s credentials to apply Group Policy / User Configuration.

Network Logons
Documents all authentications to domain controllers by users. Note that whenever such a user logs onto their own workstation or member server, this will generate a Network logon to a DC since the user’s workstation must access the domain controller under the user’s credentials to apply Group Policy / User Configuration.

Logon Failures

Windows 2003 and earlier
672, 675, 676, 680, 681

Windows Vista, Windows 2008 and later
4768, 4771, 4776

Network Logons

Windows 2003 and earlier
672, 673, 680

Windows Vista, Windows 2008 and later
4768, 4769, 4776
Logons By Type
Documents all logons to monitored servers. It provides the following:

- Complete record of all attempts to access the computer, regardless of the type of account used
- Type of logon and logon process
- IP address and name of the client computer

<table>
<thead>
<tr>
<th>Logons By Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 and earlier</td>
</tr>
<tr>
<td>528-537, 539, 540</td>
</tr>
<tr>
<td>Windows Vista, Windows 2008 and later</td>
</tr>
<tr>
<td>4624, 4625</td>
</tr>
</tbody>
</table>

Filter Events by Severity
Due to the high volume of events generated by Windows, this feature may record a large number of events. You can set the "Severity" option to "Audit Failures Only" to reduce the number of events that are captured by this feature. If you are required by law to capture this data, then verify with your compliance officer (and/or audit requirements) to ensure that you can change this setting and still remain compliant.

Collect Logons by Computer Accounts
Network logons by computer accounts can account for a large number of records in the database and dilute reporting. Uncheck the box to ignore any audit events which originate from computer accounts.

Perform additional host name or reverse lookup through DNS
When the logon id contained in the logon event (only applies to audit success events) can be linked (correlated) to an earlier logon session, then EventSentry will include the IP address and/or host name. In the case that only the host name or IP address are available, a DNS (reverse) lookup will be performed to gather the missing information.

Due to the nature of DNS lookups, this information might not 100% accurate and should not be solely relied upon.

Logon GUIDs
Captures the logon GUID available in some logon events and includes it in the search results. Capturing Logon GUIDs is generally not necessary as it provides little benefit for forensic analysis but can significantly degrade the performance of the collector in networks that generate a lot of logon GUIDs in a short amount of time.

5.6.5 Print Tracking
Print Tracking records print jobs in a central database and monitors print usage on workstations and print servers. The collected information can be queried through the web reports to obtain information such as

- How many documents and/or pages where printed on a particular printer
- Which documents where printed on a printer
- Accumulative information such as how many documents where printed by each user

Requirements
This feature works by intercepting Informational events that are written to the application event log when "Log Spooler Information Events" is enabled in the Print Server Properties of the monitored host. As
such, some requirements need to be met before print tracking can function properly. Please see Requirements for details.

Windows records print activity on the host where the print queue is located. As such, print tracking works best on networks where printers are shared on servers or dedicated print servers.

EventSentry can also track printing activity from printers directly attached to workstations. In this scenario, the EventSentry agent will need to be installed on all computers where printers are attached to.

Collected Data
EventSentry will collect the following print information on all supported Windows platforms:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date / Time</td>
<td>Date and time when the print job was submitted</td>
</tr>
<tr>
<td>Print Server</td>
<td>The computer where the print queue is located, usually the print server</td>
</tr>
<tr>
<td>Print Queue</td>
<td>The name of the printer (queue)</td>
</tr>
<tr>
<td>Document</td>
<td>The name of the document printed</td>
</tr>
<tr>
<td>Document ID</td>
<td>The ID of the document printed, a number that is increased by one every time a new document is printed.</td>
</tr>
<tr>
<td>Username</td>
<td>The name of the user who submitted the print job</td>
</tr>
<tr>
<td>Pages</td>
<td>The number of pages printed</td>
</tr>
<tr>
<td>Size</td>
<td>The total size of the print job</td>
</tr>
</tbody>
</table>

Privacy
Since collecting print information does track a users activity to some extend, you will still need to make sure that collecting this information does not interfere or violate any corporate policies or laws in place.

Configuration

Tracking All print jobs (with exceptions)
Select "Track all except those listed below" to monitor all print jobs. To exclude certain users and/or documents, click the + button and specify the username or document to exclude.

To exclude a document from being tracked, enter either the complete document name or specify part of the document name (make sure to include * when wildcard support is enabled, e.g. *manual.doc) in the Document field. Enter a * for the username if you wish to exclude this document for all users.

To exclude a user from being tracked, enter either the complete username (DOMAIN\User) or part of the username (e.g. *User1). Enter a * for the document if you wish to exclude all documents of this user.

Tracking only selected print jobs
Select "Only track listed below" and click the + button to add users/documents (see previous paragraph) that should be tracked to the list.
Enabling Print Tracking in the OS
Since print tracking needs to be enabled in the Operating System you can configure the agent to activate it automatically if it isn’t already activated. Please see requirements for more information.

Database
Select a database action where the logon data should be stored.

5.6.5.1 Requirements
The print tracking feature works by intercepting Information events that are written to the application event log when Log Spooler Information Events is enabled in the Print Server Properties of the monitored host. As such the following requirements exist:

1. “Log Spooler Information Events” must be enabled. You can have the EventSentry agent automatically enable print tracking when the service starts by selecting "Enable information events in print spooler" from the Print Server Properties.

2. To enable “Print Tracking / Auditing” without EventSentry:

Windows 2003 and earlier
Navigate to Start -> Settings and click or double-click the Printers (and Faxes) icon. Select “Server Properties” from the “File” menu. There, click on the “Advanced” tab and check the box next to "Log information spooler events". You might have to restart the “Print Spooler” service.

Windows Vista and later (incl. Windows 2008)
Open the "Event Viewer" and navigate to "Application and Services Logs -> Microsoft -> Windows -> PrintService -> Operational". Right-click "Enable Log" to start logging of print events. To disable logging again, right-click "Operational" and select "Disable Log".

3. The application event log "Log Size" needs to be configured to "Overwrite events as needed", it also recommended to specify a size of at least 2048kb. The EventSentry agent will write an error message upon startup to the application event log if the event log is not correctly configured.

You can change the “Log size” settings by opening up “Event Viewer” (from Administrative Tools) and right-clicking “Application Log”. Select "Properties" from the menu and verify that the "Log size" is correctly set to "Overwrite events as needed". Also verify that the “Maximum log size” is sufficiently big.

5.6.6 File Access Tracking

File Access Tracking collects all successful file access activity that is logged by the Operating System when auditing on a directory and/or file is enabled. File Access Tracking can report on

- files being added to a directory
- files being deleted from a directory
- files being modified
- other file changes such as permission or ownership changes

In addition, file access tracking can include the following information about a file change:

- The username of the user who performed the action
- The computer and/or IP address from which the action was performed (optional)
- The process which performed the action (unless performed through a file share)

Please see File Monitoring vs. File Access Tracking for a comparison between File Access Tracking and File Monitoring.

File Access Tracking works by intercepting and normalizing event 560 (on computers running Windows 2003 and earlier) or event 4663 (on computers running Vista and later) and performing additional actions to obtain extended information about the events (such as the source computer) and categorize the file access action.

Using File Access Tracking on Windows 2003 and earlier

One problem with the 560 security events on Windows 2003 and earlier, is that they log not just when changes are made to files, but also when changes are requested to files. Microsoft® introduced so-called operational events with Windows 2003 (event id 567), which attempt to address this problem by only logging actual file changes to the security event log. We have found the operational events to be somewhat unreliable on Windows 2003 however, in particular when files are accessed through a file share over a network. We discussed this issue in detail in our event log blog. As such, the file access tracking feature will not utilize the 567 events on Windows 2003 and earlier, they are however utilized on Vista, Windows Server 2008 and later.

To compensate for this limitation, EventSentry can manually verify certain file actions by performing additional verification on files, such as creating checksums when files are modified and verifying that files are indeed deleted. This feature is called Verify, is optional and can be activated if you are tracking file access on Windows Server 2003 (and earlier) hosts.

Using File Access Tracking on Vista, Windows Server 2008 and later

If you are tracking file access on Windows Server 2008 (this includes file accessed from remote computers through file shares), then EventSentry will intercept and normalize operational events.
making the additional processing through the **Verify** feature by the agent (as described earlier) unnecessary in most scenarios.

### 5.6.6.1 Prerequisites

In order to use file access tracking, auditing needs to be configured on the files and/or folders you would to track with EventSentry. Additionally, object tracking needs to activated either through group policy or through the local security policy.

1. **Enable Object Tracking**
   See [Tracking Requirements](#) for more information on how to enable the object tracking audit category. If object tracking is not enabled, then the necessary 560 or 4663 events will not be generated by the Operating System, even when auditing is enabled on a directory.

2. **Setup Auditing for a file and/or folder**
   Once object access tracking has been enabled, you will need to configure auditing on the directories you want to track with EventSentry. You configure auditing by accessing the folder properties in Windows explorer and accessing the advanced security properties as shown in the screenshots below:

   ![Viewing current file/folder permissions](image)

   ![Enabling auditing for file changes and deletions](image)
List of auditing entries after EVERYONE was added

The detailed steps to enable auditing are as follows:

1. Right-click the folder where you want to enable auditing, and select “Properties”
2. Click the “Security” tab
3. Select the “Advanced” button
4. Select the “Auditing” tab
5. Click “Edit”
6. Click “Add”
7. In the selection dialog, specify the user(s) and/or group(s) you would like to audit. To audit everybody, enter Everyone
8. In the “Auditing Entry” dialog, specify the type of Access you want to audit, e.g. “Create files / write data”
9. Click OK several times to confirm your selection

Auditing entries will be effective immediately.

5.6.6.2 Setting up File Access Tracking

Once auditing has been configured on one or more directories, then you can either choose to monitor one or more specific directories with EventSentry, or simply intercept all file access tracking events and normalize them.

Event Analysis

When setting up file access tracking, you need to determine at which detail level you would like to analyse events. You can either Normalize events, Normalize & Verify or Normalize, Verify & Filter events.
Normalize Only
This is the least resource-intensive option, which intercepts object tracking events, normalizes them and writes them to the EventSentry database. When setting this option, no additional verification on the files being accessed is being performed. This is the only option available when using the Track all file access activity.

Normalize Only is the recommended setting for computers running Vista and later, since those computers already generate operational events.

Normalize & Verify
This option, in addition to simply normalizing events as described above, also performs additional verifications on the files being accessed. This option requires more resources, since it creates a checksum for every file in the monitored directories as well as for any file being written to.

Verify attempts to determine most file modifications:

1. Write access to files is being verified using SHA checksums of the files
2. File deletions are being verified by checking for the non-existence of the files
3. File additions are being verified by checking for the existence of the files

If an action can be verified, then the event is flagged as "verified".

The Verify option is only available when you specify one or more directories, since it requires the agent to initialize every monitored directory.

Normalize, Verify & Filter
This selection is identical to the Normalize & Verify setting, except that only file modifications that have been verified (e.g. through a checksum) will be logged to the database. If an action was not verified, then the event will be discarded.

This option is not recommended for security-sensitive environments, since important events might be discarded when an action cannot be properly determined.

Tracking directories
You can either track all file access activity, or specify one or more directories to be monitored.

Tracking all file access activity
Select this option to track all object tracking events that are being generated on a system. When selecting this option, Event Analysis is automatically set to Normalize Only.

Monitoring one or more directories
Add one or more directories to the list to only track file access events from selected directories. You will also need to select this option to use the "Normalize & Verify" or the "Normalize, Verify & Filter" option. Click the plus icon to add a directory to the list of monitored directories. Monitoring a UNC path or network share (such as \SERVER1\Payroll) is not supported.

Additionally, you can configure which access masks should be recorded (e.g. only WriteData or Delete) and also specify a file filter to include only certain files or exclude files that should not be tracked. See Access Masks & Filter for more information.

Retrieve Source IP address and Computer Name
When the logon id contained in the file access tracking event can be linked (correlated) to an earlier logon session, then EventSentry will include the IP address and/or host name. In the case that only the host name or IP address are available, a DNS (reverse) lookup will be performed to gather the missing information.

Due to the nature of DNS lookups, this information might not be 100% accurate.
5.6.6.3 Access Masks & Filter

You can specify which types of file access are being tracked to ensure that only relevant events are being recorded in the database. Additionally, you can setup file filters to include or exclude files that match a pattern.

**Access Masks**

Windows distinguishes between the following access masks when recording file access activity, either through regular or operational events:

- ReadData
- ReadAttributes
- ReadEA
- SetPermissions
- SetOwner
- WriteData
- WriteAttributes
- WriteEA
- AppendData
- Delete
- AppendData

For example, to track when users change files, make sure that **WriteData** and **AppendData** are both selected. To record when files are deleted, make sure that **Delete** is checked.

**File Filter**
The default filter ("Include") includes all files but lets you specify exclusion on a by case basis. For example, you could exclude all files that have a tmp extension by specifying the following filter:

```
*.tmp
```

File names and paths need to be specified relative to the monitored folder. For example, if you are monitoring the folder C:\Logfiles, but want to exclude any file in the Temp sub directory (C:\Logfiles\Temp), then you would need to specify the filter as Temp\*. *

**Process Filter**

File activity triggered by specific processes can be excluded from being tracked with the process filter. Specify either the full path to the process or use a wildcard character, for example:

```
*filescanner.exe
```

C:\Program Files\FileScannerSoftware\filescanner.exe

Multiple processes can be separated with commas.

Excluding a process only works if the process in question directly accesses the files (and not via a network share) and is listed on the 4663 events. As such, processes running on clients accessing remote files cannot be excluded, since the server/host accessing the files is not aware of those (remote) processes.

**5.6.7 Account Management Tracking**

Account management tracking intercepts events related to the creation, modification and deletion of user accounts, groups and computer accounts. Depending on the type of computer this feature is being used, either local or domain accounts will be tracked.

**User Account Management**

**User Creation & Deletion**
Tracks when user accounts are created or deleted.

**User Account Modifications**
Tracks when user accounts are modified, e.g. when a password is set.

**User Status Changes**
Tracks user status changes, e.g. when a user account is disabled or enabled.

**User Account Management**

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Windows XP, Windows 2003 and before</th>
</tr>
</thead>
<tbody>
<tr>
<td>624, 626, 628, 629, 630, 642, 644, 671</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event IDs</th>
<th>Windows Vista, Windows 2008 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>4720, 4722, 4724, 4725, 4726, 4738, 4740, 4767</td>
<td></td>
</tr>
</tbody>
</table>

**Group Management**

**Group Addition & Deletion**
Tracks when groups are created or deleted.

**Group Modifications**
Tracks when groups are modified, e.g. when a global group is changed to a universal group.

**Group Membership Changes**
Tracks changes to the group membership, e.g. when members are added or removed from a group.

**Security-Enabled Groups, Distribution Groups**
Lets you configure which types of groups should be monitored.

**Computer Account Management**

**Computer Account Creation & Deletion**
Tracks when computer accounts are added or deleted.

**Computer Account Modifications**
Tracks changes to computer accounts, such as when the password of a computer account is changed.

Note: Computer account changes only occur on domain controllers.

**Retrieve Source IP Address and Computer Name**
When the logon id contained in the account management event can be linked (correlated) to an earlier logon session, then EventSentry will include the IP address and/or host name. In the case that only the host name or IP address are available, a DNS (reverse) lookup will be performed to gather the missing information.

Due to the nature of DNS lookups, this information might not be 100% accurate.

### 5.6.8 Audit Policy Monitoring
Continuously queries the current audit policy so that the current audit status of every monitored system is available in the web reports. Policy Change Tracking also intercepts various events related to policy changes, such as the change of a domain password policy or the assignment of a user right.

**Policy Changes**
Tracks all policy changes, including:

- Domain Policy Changes (e.g. password policy changes)
- Audit Policy Changes
- Kerberos Policy Changes

#### Event IDs

<table>
<thead>
<tr>
<th>Policy Changes</th>
<th>Event IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 and earlier</td>
<td>612, 617, 643</td>
</tr>
<tr>
<td>Windows Vista, Windows 2008 and later</td>
<td>4719, 4713, 4739</td>
</tr>
</tbody>
</table>

#### User Rights Changes
Tracks when user rights are assigned to or removed from user accounts, e.g. the "Create a pagefile" right.

#### Event IDs

<table>
<thead>
<tr>
<th>User Rights Changes</th>
<th>Event IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 and earlier</td>
<td>608, 609</td>
</tr>
</tbody>
</table>
Logon Rights Changes
Tracks when logon rights are granted or removed from user accounts, e.g. the “Logon as a service” right.

Trust Relationship Changes
Tracks all changes to trust relationships, including the creation, modification and removal of trust relationships.

Retrieve Source IP Address and Computer Name
When the logon id contained in the monitored event can be linked (correlated) to an earlier logon session, then EventSentry will include the IP address and/or host name. In the case that only the host name or IP address are available, a DNS (reverse) lookup will be performed to gather the missing information.

Due to the nature of DNS lookups, this information should be used with caution and might not be 100% accurate.

5.6.9 Registry Change Tracking
Intercepts Windows audit events pertaining to the Windows Registry and makes them available in the web-based reporting.
Requirements: This feature works by intercepting Audit Success events with event ID 4657 that are written to the security event log when registry auditing is enabled (either in the local security policy or via AD) and at least one registry key is configured for auditing. See requirements for details.

Collected Data
The following registry information is collected on all supported Windows platforms:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Added, Removed or Modified</td>
</tr>
<tr>
<td>Registry Path</td>
<td>Path of the value that was added, removed or modified, always starts with \REGISTRY\</td>
</tr>
<tr>
<td>Registry Value</td>
<td>Name of the registry value that was added, removed or modified</td>
</tr>
<tr>
<td>Value Before</td>
<td>Value before the change</td>
</tr>
<tr>
<td>Value After</td>
<td>Value after the change</td>
</tr>
<tr>
<td>Type Before</td>
<td>Type of the value before the change</td>
</tr>
<tr>
<td>Type After</td>
<td>Type of the value after the change</td>
</tr>
<tr>
<td>Caller Path / File</td>
<td>Processes that initiated the change, ignore for changes that were initiated remotely</td>
</tr>
<tr>
<td>Username</td>
<td>User who initiated the change</td>
</tr>
<tr>
<td>Logon ID</td>
<td>Logon ID of the session that made the change</td>
</tr>
<tr>
<td>Event #</td>
<td>Event number of the event describing the change</td>
</tr>
</tbody>
</table>
General Filter
Determines which registry activity will be picked up.

Registry Paths
Configure whether all registry changes that are audited by the Operating System are processed by EventSentry (Monitor everything), whether certain paths should be excluded ("Exclude paths listed below") or whether only select paths should be monitored ("Monitor only paths listed below").

Registry path filters need to match the format used in event 4657 and generally start with \REGISTRY\, for example:

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
\REGISTRY\USER\S-1-5-21-2574282233-618468577-1958264051-1122\Software\Microsoft\Windows\CurrentVersion\Run

When in doubt prefix the registry path with an asterisk, for example
*\Software\Microsoft\Windows\CurrentVersion\Run

Sub folders are automatically monitored.

Processes
Configure whether registry activity from all processes should be processed ("Any process"), whether certain processes should be excluded ("Exclude Processes listed below") or whether only specific processes should be monitored ("Monitor only processes listed below").

5.7 Validation Scripts

Validation scripts packages utilize validation-type scripts to verify that the OS configuration or current state of monitored hosts follows best practices and/or passes security and compliance requirements.

EventSentry includes 100+ scripts (checks) which are maintained & updated by NETIKUS.NET ltd (aka "Managed Scripts"), that can be utilized to perform a wide variety of checks including:

- STIG
- CMMC
- CIS
- NIAP
- MITRE
- NIST 800-53
- CCE
- General System Health
- Best Practices

Managed scripts are maintained & updated on a regular basis, updates are available to evaluation users and customers with active maintenance agreements. Users can supplement managed scripts with their own, managed scripts cannot be modified however.

Scripts are organized using tags, and users can supplement built-in tags with their own to make assigning scripts easier.

Configuration

Assigned Tags & Scripts
A Validation Scripts package allows users to associate existing validation scripts either by a matching tag or script GUID to be executed on all hosts which have the package assigned. Results can be stored in one or more database actions.
**Blocked Scripts**

If one or more scripts should not be included in the package, despite matching the specified tags, it can be blocked in the “Blocked Scripts” section. This can be helpful for checks that cannot be remediated or that are not applicable to the affected hosts.

Results from validation scripts are available in the web reports, no events are generated by this feature. Web-based reporting provides summary statistics, individual script results and remediation steps for failed checks.

Script can be disabled in the Scripts section to prevent them from running anywhere regardless of tag assignments. The frequency at which scripts are run is also configured in the scripts section.
Environment Monitoring

EventSentry can monitor temperature, humidity, motion, smoke and water through external sensors attached to the serial port. The hardware sensors are sold separately and can either be obtained from https://store.netikus.net (if you are located in the US) or directly from PCMeasure in Germany if you are located outside the US.

The following features are available and are configured through the Environment option of the management application. All alerts generated by the environment monitoring feature are written to the Application event log.

EventSentry currently only supports sensors from PCMeasure, and some of the supported sensors require additional hardware. The table below outlines the requirements:
<table>
<thead>
<tr>
<th>Sensor Description</th>
<th>Manufacturer Model Number</th>
<th>Connectors on sensor</th>
<th>Requires USB port</th>
<th>Requires serial port</th>
<th>Requires adapter (RJ-45 to serial)</th>
<th>Requires driver software (included)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature / Humidity (serial port)</td>
<td>30106</td>
<td>9-pin serial, USB</td>
<td>yes, for power</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Temperature / Humidity (USB)</td>
<td>30602</td>
<td>USB</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Temperature</td>
<td>30101</td>
<td>RJ-45</td>
<td>yes, for power</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Humidity</td>
<td>30103</td>
<td>RJ-45</td>
<td>yes, for power</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Water</td>
<td>30115</td>
<td>RJ-45</td>
<td>yes, for power</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Smoke</td>
<td>30111</td>
<td>RJ-45</td>
<td>yes, for power</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Motion</td>
<td>30114</td>
<td>RJ-45</td>
<td>yes, for power</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

On all sensors/adapters except for sensor 30602, the USB connectors are only used to draw power. Data from the sensors is transmitted via the serial port. In order to use the sensors, you have to connect both the USB and the serial connector.

For sensors requiring adapters (see right column "Requires adapter"), the following serial adapters exist. Each adapter as one 9-pin serial and one USB port, as well as one or more RJ-45 connectors to connect the actual sensors.

<table>
<thead>
<tr>
<th>Adapter Description</th>
<th>Manufacturer Model Number</th>
<th>Number of RJ-45 connectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-port serial adapter</td>
<td>30201</td>
<td>1</td>
</tr>
<tr>
<td>2-port serial adapter</td>
<td>30203</td>
<td>2</td>
</tr>
<tr>
<td>4-port serial adapter</td>
<td>30205</td>
<td>4</td>
</tr>
</tbody>
</table>

Sensor connected to the serial adapters must be unique; you cannot currently attach one sensor type more than once on the same computer. You can only connect one 4-port serial adapter at one time.

**Temperature Monitoring**

- Alert when the temperature is outside a configured range
- Record temperature in database for historical analysis in the web reports
- Fahrenheit / Celsius support

**Temperature + Humidity Monitoring**

- Alert when the humidity is outside a configured range
- Record humidity in database for historical analysis in the web reports

**Motion Sensors**

- Alert when motion is detected
- Records motion activity in database
- Requires serial adapter
Smoke Sensor
The smoke sensor is attached to the serial port and can alert you whenever smoke is detected.

Water Sensor
The water sensor is attached to the serial port and can alert you whenever water is detected.

Please see the next chapter for more information on the configuration of various sensors.

5.8.1 Temperature / Humidity
Temperature and humidity monitoring are configured by clicking on the Environment container.

**General Settings**
Configures the serial port where the sensor is attached to and sets the desired temperature scale. Depending on the type of sensor, one can either monitor the temperature, humidity or both.

Select the type of sensor which is attached, "Serial" by default. USB-only sensor 30602 is the only sensor which supports the "USB" selection for type (see below for details).

When attaching a temperature or a humidity sensor, then the respective position on the serial adapter to which the sensor is attached needs to be selected. The position is indicated on the actual adapter and is always 1 if the adapter only supports one sensor.

When attaching a temperature and humidity combo sensor, then both position fields are grayed out since this sensor always uses position 1 & 2 internally.
The USB-only temp/humidity sensor (30602) and serial temp/humidity (30106) sensor cannot be connected to the same host at the same time.

Important Information for USB-Only Sensor
When switching the type from "Serial" to "USB", the management console will attempt to automatically installed the required virtual COM port drivers from FTDI. These drivers emulate a serial port and are required for the sensor to work correctly. The drivers are WHQL certified, and the installation does not require a reboot. The driver installer is ftdichip_environment_usb_com_driver.exe, and is located in the resources sub directory of the installation directory. If the automatic installation does not work, then the driver can be installed manually from the command prompt by running ftdichip_environment_usb_com_driver.exe.

For more information on the USB sensors, including uninstallation instructions, see http://www.ftdichip.com/Support/Documents/InstallGuides.htm.

Calibration
In some cases it may be necessary to correct the temperature and/or humidity of the sensor, for example if the sensor is placed in a location where the temperature measured does not accurately reflect the temperature of the rest of the room. Clicking the calibrate button allows the user to either add or subtract to/from every reading reported by the sensor.

Current Measurements
If a sensor is connected to the local machine, then these two bars will show the last temperature and/or humidity reading as it was reported by the agent.

Limits
Temperature and Humidity alerts write an error event to the event log whenever the measured value falls outside your configured range, and will log an information event to event log when the measured value is back in the configured range, thus clearing the alert.

Enable Temperature Alerts: Alerts when the temperature falls outside a configurable range, alerts are generated as soon as the measured temperature falls outside the desired range.

Specify 0 for the lower end of the range if no minimum value should be set.

Enable Humidity Alerts: Alerts when the humidity falls outside a configurable range, alerts are generated as soon as the measured humidity falls outside the desired range.

Specify 0 for the lower end of the range if no minimum value should be set.

Notify me at most every XX: Configure how often an error should be written to the event log when the temperature and/or humidity fall outside the configured range.

Embedded Charts: When temperature alert events are emailed by EventSentry, they will automatically include a PNG chart from the environment data collected during the last 24 hours. The image will include the host name, the type of environment data that is charted (e.g. temperature in degrees Fahrenheit) as well as the description, if configured. The chart includes an automatically calculated trend line in orange.
### Database
In addition to being notified when thresholds are exceeded, you can also log the current temperature and/or humidity to a database to view trends and the history.

Select the database action where to write the history to and how often the current data should be written to the database. The minimum time interval is 5 minutes.

### Location
If you are using temperature/humidity sensors in multiple locations in your organization, then you can specify the location here. The location is included in the alerts that are logged to the event log, it is not shown in the web reports.

#### 5.8.2 Motion Monitoring
Motion monitoring is configured on the "Motion Sensor" tab of the Environment container.
**Connection Settings**
Select the serial port to which the serial adapter is attached to, and indicate at which position (1-4) the sensor is attached to. The position is indicated on the actual adapter and is always 1 if the adapter only supports one sensor.

**Alert Settings**
How often alerts should be generated when continuous motion is being detected.

**Database**
Select the database action to which motion information should be written to, and specify how often data should be added to the database when continuous motion is being detected.

**Location**
If you are using multiple motion sensors in your organization then you can specify the location here. The location is included in the alerts that are logged to the event log, it is not shown in the web reports.

### 5.8.3 Smoke / Water
Smoke & Water monitoring are configured on the “Smoke” and/or “Water” tab of the *Environment* container.
Connection Settings
Select the serial port to which the serial adapter is attached to, and indicate at which position (1-4) the sensor is attached to. The position is indicated on the actual adapter and is always 1 if the adapter only supports one sensor.

General Settings
Select how often you want alerts to be generated when continuous smoke or water is being detected.

Location
If you are using multiple smoke or water sensors in your organization then you can specify the location here. The location is included in the alerts that are logged to the event log, it is not shown in the web reports.

5.8.4 Event Logs
The following events are logged by the environment monitoring features with the Environment Sensors event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Severity</th>
<th>Event Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10903</td>
<td>Error</td>
<td>No environment monitor found</td>
<td>EventSentry was unable to find a temperature and/or humidity sensor on serial port COM1. Please make sure the device is connected properly.</td>
</tr>
<tr>
<td>10904</td>
<td>Error</td>
<td>Database interval too small</td>
<td>The database write interval for environment monitoring is set too small. The interval was automatically adjusted to 900 seconds.</td>
</tr>
<tr>
<td>10908</td>
<td>Error</td>
<td>The temperature has fallen outside the configured range.</td>
<td>The current temperature has fallen outside the configured range (60°F to 76°F). The current temperature is 83.58 degrees (F).</td>
</tr>
<tr>
<td>10909</td>
<td>Error</td>
<td>The humidity has fallen outside the configured range.</td>
<td>The current humidity has fallen outside the configured range (10% to 60%). The current humidity is 9%.</td>
</tr>
<tr>
<td>10910</td>
<td>Information</td>
<td>The temperature is back inside the configured range.</td>
<td>The current temperature is back in the configured range (60°F to 76°F). The current temperature is 74.57 degrees (F).</td>
</tr>
<tr>
<td>Event Code</td>
<td>Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>10911</td>
<td>Information</td>
<td>The humidity is back inside the configured range.  The current humidity is 12%.</td>
<td></td>
</tr>
<tr>
<td>10912</td>
<td>Error</td>
<td>Motion detected Motion sensor (Server Room ABC) detected motion.</td>
<td></td>
</tr>
<tr>
<td>10913</td>
<td>Error</td>
<td>Smoke detected Smoke sensor (Server Room ABC) detected smoke.</td>
<td></td>
</tr>
<tr>
<td>10914</td>
<td>Error</td>
<td>Water detected Water sensor (Server Room ABC) detected water.</td>
<td></td>
</tr>
<tr>
<td>10915</td>
<td>Error</td>
<td>Smoke sensor failed self test EventSentry failed to detect the required self-test of the smoke sensor which is run every 24 hours. Please press the TEST button on the smoke sensor for at least 30 seconds to make sure that the sensor works correctly and an alert is generated by EventSentry.</td>
<td></td>
</tr>
<tr>
<td>10916</td>
<td>Error</td>
<td>Sensor error The attached Water sensor reported an error, or no sensor is attached. This feature has been turned off.</td>
<td></td>
</tr>
</tbody>
</table>

5.9 **Heartbeat Monitoring**

Heartbeat monitoring monitors any network device that is reachable through TCP/IP. Heartbeat monitoring itself is performed through the **EventSentry Heartbeat Monitor** service and is usually installed on one computer on your network.

Heartbeat monitoring pings remote hosts and checks TCP ports, but can also query information from remote SNMP agents to obtain information like disk space, system info, uptime and performance information.

1. **Selecting computers to be monitored and setting a group type**

   In order for a computer to be monitored it will need to be added or imported into a group that is heartbeat-enabled (more info).

2. **Setting global heartbeat configuration options**

   Some configuration options (such as the polling interval) will be set globally, applying to all computers. Other options can be set on a per-group and on a per-host level (more info).

3. **Setting group options**

   This chapter shows how to setup the initial monitoring configuration for a group (more info).

4. **Customizing heartbeat options on a per-host basis**

   This chapter explains how to override group settings on a per-host level (more info).

5. **Setting maintenance schedules for schedules outages**

   If one or more machines are schedules to be down at a certain day or hour then you can set maintenance schedules for these periods to avoid receiving notifications (more info).

6. **Viewing the heartbeat status and history through the web reports**

   The current heartbeat status is available under “Status - Heartbeat” in the web reports.

5.9.1 **SNMP / SSH Monitoring**

The Heartbeat Agent utilizes **SNMP (v1, v2c & V3)** and **SSH** (when available) on the remote host to gather more information from the monitored device.

Using **SNMP** the following information can be retrieved:

- Disk Space information
- Performance Monitoring
- Hardware Summary
Monitoring with EventSentry

- Running processes (alerting only)

Using SSH the following information can be retrieved:

- Extended system information (time zone, USB version, BIOS, OS install date, extended CPU info
- Running daemon / services

**Automatic Detection**
The heartbeat agent will attempt to detect certain features on a remote host automatically and retrieve the associated information via SNMP or SSH.

**VMWare ESXi**
When VMWare is detected on a remote host, a VM inventory is retrieved from the remote host and available on the **Inventory - Virtual Machine** page. The following details are available:

- Product Name
- Product Version
- Product Build
- VM Name
- Current VM status
- VM Operating System (if tools are installed)
- Assigned CPUs
- Assigned memory
- Path to .vmx file

**MAC to Switch Port Mapping**
If the monitored device is a switch, the MAC address to switch part mappings are automatically retrieved and available on the **Inventory - Switch** page. The MAC addresses are correlated to hardware information obtained by the agents and the ARP daemon so that host names can be displayed whenever possible.

**Logging**
The SNMP capabilities of a remote device are determined automatically when the heartbeat agent initializes after startup, and event 11020 is logged for every device which supports at least SNMP v1.

All features require that the respective system health object (e.g. disk space, performance monitoring) is assigned to the monitored hosts.

If no disk space, performance or software/hardware inventory object is assigned to a host, it will not be monitored via SNMP.

**Error Handling**
EventSentry suspends SNMP monitoring of a host under the following conditions:

1. The Heartbeat Service is unable to query a remote host via SNMP during the first monitoring interval after service startup.
2. The Heartbeat Service is unable to query a remote host via SNMP for more than 24 hours, event id 11023 will be logged and SNMP monitoring will be disabled for the host.
3. The Heartbeat Service is unable to query a remote host via SNMP at least 50% of the time during a 48-hour period, event id 11015 will be logged and SNMP monitoring will be disabled for the host.

To re-enable SNMP monitoring, follow the instructions in the logged event or open the management console, locate & click the host inside its respective computer group and finally click the SNMP-related warning to re-enable SNMP monitoring.
5.9.2 Adding Computers

Selecting Group Features
Before adding computers to an existing or new group, the appropriate group features need to be selected. The group features determine whether computers in a group will be monitored by the heartbeat monitor or not. Group features are configured by toggling the check boxes in the “Group Features” section.

The following group types are available:

- **Manage EventSentry agents**
  Enables the management of computers in this group through the Remote Update feature. This supports installing, uninstalling and updating EventSentry agents on all computers in this group.

- **Monitor Heartbeat (ping, TCP status)**
  Monitors all computers/devices in this group with the Heartbeat Agent. Note that the option to “Monitor EventSentry agents” is only available if the first check box is also checked.

  **Note:** At least one check one of the two check boxes needs to be checked.

Adding or Importing Computers
Computers can either be added manually by right-clicking the Computers container of a particular group, or imported through a variety of ways, see Remote Update -> Importing for more information on importing computers.

When linking a group to Active Directory, be sure to click “Get Service Status” once (right-click the computers container) so that the computers from Active Directory are cached.

You will also need to select “Get Service Status” or restart the management console every time the list of computers change in Active Directory.

5.9.3 Global Options

Global heartbeat options are configured in the Heartbeat container where a variety heartbeat monitoring options that affect all hosts regardless of group membership are configured.
General

Monitoring Interval: This interval determines how often the monitored computers are being polled, in seconds.

Thread Management: The heartbeat agent uses threads to scan hosts in parallel. When set to automatic, the agent automatically calculates the number of threads to use based on the number of hosts that are being monitored as well as the time it takes to monitor the hosts. Depending on the actual scan speed, the agent will dynamically adapt the thread count and increase or decrease the thread count as needed. When set to manual, the agent will always use the number of threads specified in "Max # of threads", regardless of the number of hosts and scan speed. Regardless of this setting, the agent will never use more threads than there are hosts to monitor.

Max # of threads: With thread management set to automatic, specifies the maximum number of threads (upper limit) the agent will use. With thread management set to manual, specifies the number of threads the agent will use.

Event Log Logging
Logging Status Changes: You can optionally write status changes to the event log, so that you can be notified if a certain computer or service becomes unavailable. A positive status change applies when a computer or service was previously unreachable, but is now reachable again. A negative status change applies when a computer or service was previously reachable, but is not anymore. As such it is recommend to log negative status changes at least as warnings. See Event Log for all events logged by this feature.

When host is down, notify every: By default, the heartbeat service only notifies of host status changes. That is, it will generate one event whenever a host or TCP port goes from online to offline and vice versa. When enabled, configures the heartbeat service to continuously generate an alert when a host, service or remote agent is down. The selected time interval will define how often these continuous alerts will be generated.

Notify if EventSentry service is unavailable: The heartbeat service relies on the EventSentry service to perform any immediate notifications, such as email or page notifications. This is because the heartbeat service logs all status alerts (e.g. when a host is unreachable) to the event log. As such, when heartbeat alerts are utilized, then this option should be checked so that the heartbeat service sends an email notification when the EventSentry service is not running. This option can be ignored if heartbeat information is only utilized in the web reports.

Default SSH Port: The SSH port to use when SSH credentials are configured for a host or group. SSH is only used for Non-windows hosts.

Database
Collects all data collected by the heartbeat agent in the selected database to provide current status as well as historical data. Data collected by the heartbeat agent includes:

- Current status of all monitored host indicators (ping, agent and/or TCP)
- All SNMP metrics, including performance and disk space
- System information of network devices
- VM inventory of VMWare hosts
- MAC to switch port mappings

Utilize Collector: If a collector is available and the heartbeat agent is installed on a network that does not have direct connectivity to the selected database, enabling this option will configure the heartbeat agent to send all data through the collector. This option is disabled by default and should only be enabled in MSP-style scenarios.

5.9.4 Group Options
Defines the default monitoring parameters of computers in a group, such as the required ping success rate. To set the heartbeat options for a group, simply select the group and choose "Heartbeat Options" in the context menu or ribbon.
All settings that are defined on this dialog serve as an initial default for all computers in the group. As soon as you configure (=override) the options for any particular computer individually, these settings will no longer apply to this computer.

**Default Group Database**

A default database action can be **assigned to a group**, which can then be dynamically referenced in a package. This makes it possible to configure a separate database for each group and have agents dynamically utilize that database without requiring a duplication of packages.

**Advanced Options**

- **Only check agent status or TCP ports if ping successful**: If this feature is activated and a monitored host is not reachable through PINGs, then the heartbeat agent will not attempt to check the agent status and/or TCP status, assuming that the host is down. The agent or TCP status of the host will then change to an **UNKNOWN** status.

- **Require X attempts before error**: When activated requires that a monitored feature (ping, agent or TCP port) be down for X times before an error is written to the event log. Please note that information reflected in the Web Reports is not affected by this setting, status changes will always be reflected in the Web Reports immediately.
Repeat Failed Hosts (2nd Attempt): After all hosts have been checked and it is determined that one or more services failed, then those failed services will be retried. If the 2nd scan is successful, then no error will be logged (not even to the database).

Ping Options
To enable monitoring through PING, check the Ping Hosts check box. You can then customize how ICMP packets are sent:

Packet Count: How many packets to send, default are 4.
Packet Size: The payload size of outgoing packets, default are 32 bytes.
Required Success Rate: The percent of packets need to be acknowledged for a PING to be considered successful.
Maximum Roundtrip time: The minimum required average round trip time before the status changes to error.

Collect ping stats for trending: Logs the round-trip time and packet loss percentage of ICMP packets to the database. The data is available under “Network - Response Times” in the web reports.

Agent Options
Check this box to monitor the EventSentry agent on the remote computers. If the current service state is anything other than Running, then the agent status changes to “Error”.

Starting with v3.3, EventSentry uses two methods to obtain the agent status from a remote host when the collector is disabled, three if the collector is enabled. Only if a previous method fails or is unavailable, will the heartbeat monitor move on try the next method.

1. Collector Enabled: The heartbeat monitor communicates directly with the (local) collector to determine the agent status of a remote host. Note: Requires the collector to be installed on the same host as the heartbeat monitor.
2. Database: Queries the database to determine the status of a remote host. Note: Requires that a Software/Hardware inventory package is assigned, and that the “Refresh Uptime” option is set to the lowest interval.
3. Direct: The Heartbeat service connects directly to the SCM (Service Control Manager) of the remote host and queries the “EventSentry” service.

Important information regarding authentication

If determining the remote agent status via collector and database fail, then connecting directly to the remote host is the only option for getting the EventSentry agent status. This approach however requires that the heartbeat monitor has sufficient privileges to query the remote host.

By default, the EventSentry heartbeat monitor service runs under the LocalSystem account, which only has limited access on remote computers. As such, if you intend to monitor the EventSentry agent status with the heartbeat monitor and have set authentication for a folder or computer, then you should make sure that the EventSentry Heartbeat Monitor service runs under the same account under which the authentication credentials have been set.

In a nutshell, if you are logged into the server where EventSentry was installed as user JoeAdmin and set authentication in the management console on one or more groups, then you should make sure that the EventSentry heartbeat monitor is also running under the JoeAdmin user account. Only then can the heartbeat service use that authentication information.

TCP Options
Verify whether one or more TCP ports are listening or not. You can manage the list by clicking the Edit Services ... button.
To monitor one or more ports simply select the port from the list on the left (you can select multiple ports by pressing and holding the CTRL button on your keyboard) and click the arrow button. To remove one or more ports, click the button. If a port is not listed in the list on the left, enter it manually into the edit field on the bottom left.

5.9.5 Customizing Heartbeat Settings

Once the global heartbeat options are configured, individual computer settings can be customized if necessary. For example, while you might want to ping all computers, only one computer might be running the SMTP service on TCP port 25.

Heartbeat settings can be customized in a variety of ways:

1. Right-click the host and select “Heartbeat Settings”
2. Select the host and choose “Heartbeat Settings” from the ribbon
3. Perform a “check status” on the group or all groups (see below)

To view the current heartbeat settings of all hosts in a group (or all hosts configured), select Check Status from the ribbon or by right-clicking the computers container.
The screenshot shows three hosts, with one host having customized heartbeat settings.

The letters shown in the **Options** column are abbreviations for Ping [P], Agent [A] and TCP [T]. If the letter for the particular feature is shown in the Options column, then the respective service will be monitored.

To customize the settings for a computer, right-click the host and select “Override Group Settings”. This will yield a dialog similar to the one shown below:

When you press the **OK** button, the computer will be monitored using the settings specified in the dialog. It is currently not possible to only override a particular option, for example only override the TCP option.

After you save the configuration you will need to wait for the next heartbeat monitoring interval before you will see your changes reflected on the heartbeat status page.

In order for a computer to inherit the default group settings again, click the **Use Defaults** button. This will dismiss the dialog and the computer will inherit the group settings again.
5.9.6 Defining a Host as a Router

When monitoring routers in addition to other network devices, such as servers that are located behind that router, unnecessary heartbeat alerts can be avoided by assigning the “router” flag to a monitored computer.

Routers can be defined in two ways:

- Router for all hosts in a group
- Router for one or more specific subnets

A host can be configured as a router by right-clicking the host in the left tree pane, or by selecting the host and choosing “Set as Router” from the ribbon.

When a host is designated as a router in a group, then alerts written to the event log will be suppressed for all hosts for which the router is responsible for, with the exception of the host which is designated as a router. Information that is written to the database is not affected by this setting, and the heartbeat status and history page will still show the actual network status.

**Router for all hosts in a group**
When selected, makes the host the dedicated router for all hosts in the same EventSentry group.

**Router for one or more subnets**
When selected, makes the host the dedicated router for all hosts in the specified subnet(s). For example, if the specified subnet is 192.168.8.0/24 and the dedicated router becomes offline, then event log alerts will be suppressed for all hosts in the IP range from 192.168.8.1 to 192.168.8.254 (while the router is offline). Specify the network mask in CIDR notation.

The table below shows which type of alerts will be generated when a router becomes unavailable:

<table>
<thead>
<tr>
<th>Computer</th>
<th>Router</th>
<th>Network Status</th>
<th>Event Log</th>
<th>Heartbeat Status</th>
<th>Heartbeat History</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROUTER</td>
<td>Yes</td>
<td>Host Down</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HOST1</td>
<td>No</td>
<td>Unknown</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HOST2</td>
<td>No</td>
<td>Unknown</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
5.9.7 Setting Maintenance Schedules

Maintenance schedules are useful when servers or devices that are monitored by the heartbeat agent have scheduled down-times, during which alerts should not be sent via email or pagers for example. EventSentry supports two types of maintenance schedules:

- Immediate: Puts a host immediately into a maintenance schedule either for X minutes/hours/days or until a specified time. This action can only be applied to a single host.
- Fixed schedules: You specify a start date/time and an end date/time when a device is scheduled to be offline.
- Recurring schedules: You can specify a weekday (e.g. Saturday) or day of the month (e.g. 4th) during which a device is scheduled to be offline.

Maintenance schedules can be applied to

- Individual computers
- Heartbeat-enabled groups

Maintenance schedules only affect heartbeat alerts written to the Application event log. Status changes are still added to the heartbeat history, even if they occur during a maintenance schedule.

To suppress email and/or pager alerts sent by an agent during a maintenance schedule, see Setting Maintenance Schedules for Agents.

Maintenance Now

A single host can immediately enter maintenance mode with the "Maintenance Now" feature, which can be accessed through via the ribbon or the context menu. Two maintenance options are available with this action:

- Enter maintenance mode for a number of minutes, hours or days from now.
- Enter maintenance mode until a set hour - up to 23 hours into the future. The selected time applies to the next day if it is earlier than the current time.

It is not necessary to save or push the configuration when "Maintenance Now" is specified. The configuration is saved automatically and pushed to the remote host if necessary.

![Enter Maintenance Mode dialog](image)
**Viewing maintenance schedules**
Right-click the group or computer container and select "Maintenance Schedule(s) ..."

or click the "Maintenance" button on the heartbeat options dialog of a group or computer:

**Adding maintenance schedules**
The "Heartbeat Maintenance Schedules" dialog allows you to view, add and remove maintenance schedules:
To add a regular schedule, specify the start and end date and time and click the add button. To add a recurring schedule, specify either one or more weekdays or one or more days of the month.

To cover an entire day, the start time needs to be set to **12:00:00 AM** and the end time to **11:59:59 PM**, as shown below:

![Add New Maintenance Schedule](image)

**Apply to nth weekday of the month**

Maintenance schedules can be applied to the nth day of a month only (opposed to every weekday), by selecting 1st, 2nd, 3rd, 4th or 5th from the drop-down. Select "every" for the maintenance schedule to apply to every weekday, the default setting.

**Removing maintenance schedules**

Existing maintenance schedules can be deleted by selecting it from the list of active maintenance schedules and clicking “Delete”.

### 5.9.8 Event Log

The following events are logged by the Heartbeat Agent with the **Heartbeat Monitoring** event category.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11000</td>
<td>Host %1 (%2) changed its PING status from %3 to %4. The reason for the status change was: &quot;%5&quot;.</td>
<td>Host <a href="http://www.competition.com">www.competition.com</a> (BigBrother) changed its PING status from OK to ERROR. The reason for the status change was: &quot;100% packets missing&quot;.</td>
</tr>
<tr>
<td>11001</td>
<td>Host %1 (%2) changed its AGENT status from %3 to %4. The reason for the status change was: &quot;%5&quot;.</td>
<td>Host DC1 (DomainControllers) changed its AGENT status from OK to ERROR. The reason for the status change was: &quot;Agent Stopped&quot;.</td>
</tr>
<tr>
<td>11002</td>
<td>Host %1 (%2) changed its TCP status from %3 to %4. The reason for the status change was: &quot;%5&quot;.</td>
<td>Host mail.yourdomain.com (DMZ) changed its TCP status from OK to ERROR. The reason for the status change was: &quot;Unable to establish a TCP connection (10060) (TCP Port: 25)&quot;.</td>
</tr>
<tr>
<td>11005</td>
<td>The EventSentry Heartbeat monitor is ready and will now start monitoring the configured hosts.</td>
<td>The EventSentry Heartbeat monitor is ready and will now start monitoring the configured hosts.</td>
</tr>
<tr>
<td>11006</td>
<td>The EventSentry Heartbeat agent was unable to find the required HTML template files in %1\Heartbeat. Please make sure that the following files exist in %1\Heartbeat:</td>
<td>The EventSentry Heartbeat agent was unable to find the required HTML template files in C:\Program Files\Heartbeat. Please make sure that the following files exist in C:\Program Files\Heartbeat:</td>
</tr>
<tr>
<td></td>
<td>template_status_start.html</td>
<td>template_status_start.html</td>
</tr>
<tr>
<td></td>
<td>template_history_start.html</td>
<td>template_history_start.html</td>
</tr>
<tr>
<td></td>
<td>template_end.html</td>
<td>template_end.html</td>
</tr>
<tr>
<td></td>
<td>image subdirectory</td>
<td>image subdirectory</td>
</tr>
<tr>
<td>Event Code</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>11007</td>
<td>The EventSentry Heartbeat agent was unable to find the required HTML template files and is not configured to log heartbeat status information to a database. The heartbeat agent will only notify you of host status changes through the event log.</td>
<td></td>
</tr>
<tr>
<td>11008</td>
<td>The database action specified for the heartbeat monitoring service is invalid and database logging has been disabled. Please review the configuration and restart the heartbeat monitoring service.</td>
<td></td>
</tr>
<tr>
<td>11009</td>
<td>The Heartbeat Monitor detected that the EventSentry service is currently not running. If the EventSentry service is not running, then event log alerts generated by the Heartbeat Agent cannot be forwarded to a notification. You can disable this check under &quot;Global Options -&gt; Heartbeat&quot;.</td>
<td></td>
</tr>
<tr>
<td>11010</td>
<td>The EventSentry Heartbeat service encountered an unrecoverable error and will now automatically restart. If you see this message on a regular basis, then set the &quot;Debug Level&quot; under &quot;Heartbeat&quot; to &quot;High&quot; and contact <a href="mailto:support@netikus.net">support@netikus.net</a> the next time this message is generated.</td>
<td></td>
</tr>
<tr>
<td>11011</td>
<td>Scanning of host %1 was forcefully aborted because the scan duration (%3) exceeded the maximum allowed time (%2 seconds). Review the monitoring settings of this host, and optionally disable Agent and/or TCP checks on this host.</td>
<td></td>
</tr>
<tr>
<td>11012</td>
<td>Scanning of host %1 was interrupted %4 consecutive times because the scan duration (%2) exceeded the maximum allowed time (%3 seconds). TCP Port and/or SNMP scanning may be incomplete on this host.</td>
<td></td>
</tr>
<tr>
<td>11014</td>
<td>SNMP monitoring of host %1 has failed %2 consecutive times and is now disabled. To re-enable SNMP monitoring of host %1, restore SNMP connectivity and restart the EventSentry Heartbeat Monitor service. Indicates that a host scan had to be aborted multiple, consecutive times and that its hosts status may be incomplete.</td>
<td></td>
</tr>
<tr>
<td>Event Code</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>11015</td>
<td>SNMP or agent monitoring of host %1 has failed %2% of the time over the last %3 seconds and is now disabled. To re-enable SNMP and/or agent monitoring of host %1, restore full connectivity to the remote host, locate the host in the management console and click the &quot;Retry&quot; button in the summary view. Indicates that SNMP monitoring has been permanently disabled and needs to be manually re-activated through the management console.</td>
<td></td>
</tr>
<tr>
<td>11016</td>
<td>The following error occurred while communicating, or attempting to communicate with database action &quot;%1&quot;: &quot;%2&quot;. Please verify that the database is accessible and the database is on the latest schema. Indicates an error while trying to store data in the EventSentry database. Run the configuration assistant to ensure that all database are on the latest schema.</td>
<td></td>
</tr>
<tr>
<td>11017</td>
<td>The connection with database action &quot;%1&quot; has been reestablished, the database is no longer offline. Indicates that a previously unavailable database is now available.</td>
<td></td>
</tr>
<tr>
<td>11018</td>
<td>Starting with EventSentry build 3.2.1.28, the heartbeat agent can query the EventSentry database to determine a remote agent status, instead of querying the remote agent status using the Windows API. This can drastically improve the monitoring speed and is recommended for networks consisting of 50 or more Windows hosts. Click here for more information.</td>
<td></td>
</tr>
<tr>
<td>11019</td>
<td>Monitoring of the remote EventSentry agent on host %1 has been unsuccessful %2 times in a row. Remote agent monitoring will now be disabled on host %1. Monitoring of a remote agent failed too many times and is now disabled.</td>
<td></td>
</tr>
<tr>
<td>11020</td>
<td>The heartbeat agent will monitor the following host using SNMP: Host: %1 SNMP Version: %2 System Description: %3 The heartbeat agent will monitor the following host using SNMP: Host: 192.168.73.43 SNMP Version: 2c System Description: ProCurve J9021A Switch 2810-24G, revision N.15.09, ROM N.12.03 (/sw/code/build/bass(bh7))</td>
<td></td>
</tr>
<tr>
<td>11050</td>
<td>The PING status of host %1 (%2) remains at %4 due to error &quot;%5&quot;. The PING status of host mail.somedomain.com (Heartbeat Hosts) remains at ERROR due to error &quot;100% packets missing&quot;.</td>
<td></td>
</tr>
<tr>
<td>11051</td>
<td>The AGENT status of host %1 (%2) remains at %4 due to error &quot;%5&quot;. The AGENT status of host DC1 (DomainControllers) remains at ERROR due to error &quot;Agent Stopped&quot;.</td>
<td></td>
</tr>
<tr>
<td>11052</td>
<td>The TCP status of host %1 (%2) remains at %4 due to error &quot;%5&quot;. The TCP status of host mail.yourdomain.com (DMZ) remains at ERROR due to error &quot;Unable to establish a TCP connection (10060) (TCP Port: 25)&quot;.</td>
<td></td>
</tr>
</tbody>
</table>

## 5.10 Network Services

The network services feature, which runs as a separate Windows service ("EventSentry Network Services"), contains the following components:
As such, the "EventSentry Network Services" service will need to be installed and running if any of the above mentioned components are being utilized.

1. Installing the "Network Services" service
   The service is normally installed during setup if Syslog or SNMP functionality is requested. The service can also be installed manually in the management console by navigating to "Network Services" and clicking the "Install" button.

2. Requirements
   Operating System: The correct Microsoft® Visual C++ Redistributable needs to be installed in order for the service to start, installed by default. See requirements for more information.

   Licensing: A minimum of 5-host Heartbeat / Network Device licenses need to be installed for the service to start and accept network packets. Evaluation licenses do not have this requirement.

3. Debug Level
   You can set a debug level for troubleshooting purposes, e.g. when instructed by EventSentry support. The following debug levels are available:
   - None
   - Error
   - Warning
   - Info
   - Debug
   - Trace (most)
It is not recommended to enable the debug or trace logging levels unless instructed by NETIKUS.NET support.

4. Active Components
This area shows which components inside network services are actively running. A green check mark indicates the component is active, whereas a "X" indicates that the component is inactive.

5. Database
Utilize Collector: If a collector is available and the network services are installed on a network that does not have direct connectivity to the selected database, enabling this option will configure the network services to send all data through the collector. This option is disabled by default and should only be enabled in MSP-style scenarios.

5.10.1 Syslog Daemon
EventSentry can emulate a Unix / Linux Syslog server which enables it to receive Syslog messages from remote Syslog-enabled hosts and devices. The Syslog daemon supports UDP, TCP and TCP+TLS connections and you can either log incoming Syslog messages to the application event log or store them in a database.

To activate the Syslog daemon, check one of the check boxes in the Syslog Daemons section on the "General" tab and configure either the database or event log feature.

**Syslog Daemons**
The Syslog daemon can accept UDP and TCP connections from remote Syslog-capable devices. To activate either protocol, check the appropriate check box. The default port for the Syslog protocol is 514 but can be adjusted to use a custom port.

**TCP + TLS**
Automatically creates a self-signed certificate file the first time the feature is enabled to facility TLS communication. Creates the following files:

- %SYSTEMROOT%\system32\eventsentry\secure\es_network_svc.pfx
- %SYSTEMROOT%\system32\eventsentry\secure\es_network_svc.pem (public certificate for distribution)

The public PEM file can be copied to remote Syslog clients that require this file in order to trust the self-signed certificate file.

Threshold Settings
To limit the number of Syslog messages that are processed by the Syslog daemon, change the maximum number of messages and the applicable time period. The Syslog daemon will drop incoming packets if the count exceeds the number specified in Maximum number of allowed messages for the configure Time Period.

Authorized IP Addresses / Networks
For enhanced security the Syslog daemon can be configured to only accept packets from certain IP addresses and/or networks. Host names are not allowed in the list, only IP addresses can be specified.

IP addresses can be entered with or without specifying the subnet bits. For example, to only add two servers with the IP addresses 184.23.22.11 and 184.23.22.43, simply add those two IP addresses to the list.

To authorize a whole subnet, for example the IP addresses 184.23.22.1 - 184.23.22.254, add 184.23.22.0/24. To only allow the range of 184.23.22.128 - 184.23.22.254 then specify 184.23.22.128/25.

Compatibility
The EventSentry Syslog daemon works with every Unix Syslog daemon (any Linux, Solaris, OSX, ...) and network devices that support the Syslog RFC 3164 protocol.

5.10.1.1 Database Consolidation
The Syslog daemon can be configured to write incoming packets to a database on the “Syslog to Database” tab, where one or more databases can be added to the list by clicking the “Add” button.
Settings

By default, all Syslog messages received will be sent to the specified database(s). To change this behavior, certain messages can be excluded from being added to the database (include all, exclude some), or only specific Syslog messages can be sent to the database. Manage inclusions and exclusions with the + and - icons.

**Include:** Log all Syslog messages to the database, except for exclusions below

This is the default setting, and sends all Syslog messages to the database. Syslog messages containing strings that are listed below will be filtered to reduce noise, wildcards are supported.

**Exclude:** Only log Syslog messages to the database that are included below

This setting is more restrictive and only sends Syslog messages to the database that match the filters listed, wildcards are supported.

More details on the filter syntax are explained in the "Syslog to Event Log" chapter.

5.10.1.2 Syslog to Event Log

Incoming Syslog packets can be logged to event log to facilitate real-time alerts, e.g. via email. The feature is enabled on the "Syslog to Event Log" tab with the "Log to the APPLICATION event log" check box. Since the Syslog protocol supports 8 different severities (compared to just 3 for the Windows event log), a mapping of severities needs to be configured.

EventSentry will log all messages to the application event log with event ID 500 and event source **EventSentry Network Services**.

**Severity Mapping**

Configures the mapping between Syslog severities and Windows event log severities.
Unix Syslog defines eight severity levels:

- EMERG Emergency
- ALERT Alert
- CRIT Critical
- ERR Error
- WARNING Warning
- NOTICE Notice
- INFO Info
- DEBUG Debug

The Windows event log defines only three severities (SUCCESS is not mentioned since it is basically equivalent to INFORMATION):

- ERROR
- WARNING
- INFORMATION
- Ignore (does not log message to the event log)

To prevent a certain error level (e.g. debug) from being written to the Windows event log, specify Ignore in the corresponding Windows column. This will drop all packets from the specified error level without logging them to the event log.

Settings

By default, no incoming Syslog messages will be logged to the event log. Clicking the + icon will add additional filters to the list (see below for filtering syntax and examples). Wildcards * and ? are supported.

Include: Log all messages to the event log, except for exclusions below

This setting will log all Syslog messages to the event log. Syslog messages containing strings that are listed below will be excluded.

Exclude: Only log messages to the database that are included below

This is the default setting, and only logs Syslog messages to the event log that match the listed filters.

Syntax

Syslog message filters are compared to the following Syslog format:

hostname[facility.severity]: content
ipaddress[facility.severity]: content

hostname: The host name of the remote host, if the remote IP address as was able to be resolved to a host name
ipaddress: The IP address of the remote host, if the host name could not be resolved with a reverse lookup
facility: The Syslog facility, e.g. auth, cron, kern, etc.
severity: The Syslog severity, e.g. emerg, alert, crit, etc.
content: The actual content of the Syslog message

Examples:

firewall01.prod.local[kern.crit]: Invalid login from 11.32.23.111
Example Filters
- Match all "info" severities from hosts that start with "firewall": firewall[*.*]*
- Match all messages that contain "com.apple.wikid": *com.apple.wikid*
- Match all messages from facility "local7" with severity "notice": *[local7.notice]*
- Match all messages from hosts from the 192.1.1.0/24 subnet: 192.1.1.*

5.10.1.3 Unix/Linux Configuration

Before Unix / Linux hosts can send Syslog messages to EventSentry they will need to be configured to do so. The main configuration file for most flavors of Unix is syslog.conf, usually found in the /etc directory. For Ubuntu-based systems, the /etc/rsyslog.d/50-default.conf file needs to be edited.

Because the syntax for this file is slightly different from Unix version to Unix version, EventSentry will only cover the RedHat© Linux configuration. All actions below are performed on Linux.

1. Make sure you can ping the host where EventSentry is running from your Unix / Linux box. If not, update the /etc/hosts file or ask your name service provider to make the change for you.

2. Edit the file /etc/syslog.conf and add the following line

```
*. debug              @our host name
```

you will need to format this line with the correct number of tabs

*.debug is an extreme example and will send you every single message from the Linux box. You can reduce this by choosing a higher level such as *.notice*. The syslog daemon will send you all messages from the specified level and higher, but not from the lower ones. Of course you can also specify the facility (such as kern or mail). Please see the Syslog manpage for more details on how to configure syslog.conf.

3. Restart the syslog daemon by typing /etc/init.d/syslog restart

4. Some Unix Operating Systems come with a command-line utility called logger which enables you to create your own log entries which can be very useful for testing. On Linux you can type

```
logger -p auth.notice TESTMESSAGE
```

to create a message with the content "TESTMESSAGE" for the facility auth and severity notice. Please check your Operating System documentation to see if the same or a similar utility are included. Please also note that the syntax for this command might vary on different platforms.

5.10.2 Snmp Trap Daemon

EventSentry can receive SNMP v1, v2c and v3 traps from remote network devices. The SNMP trap daemon can either log incoming traps to the application event log or store them in a database.

To activate the SNMP trap daemon, check the Enable SNMP Trap Daemon check box on the "General" tab and configure either the database or event log feature. The default SNMP port is 162, but can be changed to another port.
Threshold Settings

To limit the number of incoming traps that are processed by the daemon, change the maximum number of messages and the applicable time period. The daemon will drop incoming packets if the count exceeds the number specified in Maximum number of allowed messages for the configure Time Period.

Authorized IP Addresses / Networks

For enhanced security you will have to specify from which hosts the daemon will accept packets. Please note that host names are not allowed in the list, you can only specify IP addresses.

IP addresses can be entered with or without specifying the subnet bits. For example, to only add two servers with the IP addresses 184.23.22.11 and 184.23.22.43, simply add those two IP addresses to the list.

To authorize a whole subnet, for example the IP addresses 184.23.22.1 - 184.23.22.254, add 184.23.22.0/24. To only allow the range of 184.23.22.128 - 184.23.22.254 then specify 184.23.22.128/25.

Compatibility

The daemon should work with any SNMP compatible device that supports v1, v2c or v3.

5.10.2.1 Mibs, Communities & Users

The "Mibs, Communities & Users" tab configures which MIB files to load, which communities to accept and also configures SNMP v3 users.
Mibs
In order for OIDs to be interpreted correctly, MIBs that match the received traps will need to be configured. Which MIBs to load depends from which devices the daemon will be receiving traps from. Standard MIBs can be downloaded from the Internet, whereas vendor-specific MIBs are usually obtained from the vendor, e.g. the vendor's web site.

You can specify up to 128 MIB files, multiple MIB files can be selected when adding MIBs.

Make sure that any MIB files added are located on a physical drive, and not a network drive, and that the account the "Network Services" service is running under ("LocalSystem" by default) has permissions to read the file(s).

Communities
SNMP v1 and v2c traps use community names for authentication; specify community names for which traps should be accepted here. Traps using a community name that is not listed will be silently discarded.

SNMP v3 Users
Incoming v3 traps need to be authenticated in order to be accepted.
SNMP v3 users support the following properties:
- Username (required)
- EngineID (optional, a usually unique identifier from the network device)
- Authentication password and algorithm
- Encryption password and algorithm

Authentication and Encryption
When transmitting SNMP v3 traps over a network, you can choose to authenticate to ensure authenticity of the sender, and/or encrypt the trap to ensure that the contents of the trap are not visible to a third party. Encrypting traps is particularly important when transmitting traps over an insecure media like the Internet. The following authentication and encryption algorithms are currently supported:

Authentication: MD5, SHA
Encryption: DES, AES, 3DES

5.10.2.2 Database Consolidation
To log traps to a database, click the “Traps to Database” tab and add one or more databases to the list of databases by clicking the "Add" button.

Settings
By default, all SNMP traps received will be sent to the specified database(s). To change this behavior, you can either exclude certain messages from being added to the database (include all, exclude some),
or only send specific SNMP traps to the database. Click the + icon to add strings that will include or exclude SNMP traps.

**Include:** Log all SNMP traps to the database, except for exclusions below
This is the default setting, and it will send all traps to the database. Traps containing strings that are listed below will not be sent to the database. This allows you to conserve space in the database by filtering out unneeded messages.

**Exclude:** Only log SNMP traps to the database that are included below
This setting is more restrictive and will only send SNMP traps to the database that are listed below. This allows you to only send messages to the database that match your filters.

Add a heading and/or trailing asterisk when specifying a partial string match. When filtering traps, EventSentry will evaluate the strings you specify against the trap id, as well as the numerical OIDs, text OIDs and actual values of all trap bindings.

### 5.10.2.3 Traps to Event Log

To log SNMP traps to the event log, click the "Traps to Event Log" tab, check the "Log to the APPLICATION Event Log" check box and specify the severity under which incoming traps should be logged as.

EventSentry will log all traps to the application event log with the following event properties:

<table>
<thead>
<tr>
<th>SNMP Version</th>
<th>Event Source</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1, v2c</td>
<td>EventSentry Network Services</td>
<td>600</td>
</tr>
<tr>
<td>v3</td>
<td>EventSentry Network Services</td>
<td>601</td>
</tr>
</tbody>
</table>
**Settings**

By default, no incoming SNMP traps will be logged to the event log. Click the + icon to add strings that will trigger event log alerts.

**Include: Log all SNMP traps, except for exclusions below**

This setting will log all SNMP traps to the event log. SNMP traps containing strings that are listed below will not be logged to the event log.

**Exclude: Only log SNMP traps that are included below**

This is the default setting, and will only log SNMP traps to the event log that match the strings listed below. This allows you to only send content to the event log that matches your filters.

Add a heading and/or trailing asterisk when specifying a partial string match. When filtering traps, EventSentry will evaluate the strings you specify against the trap id, as well as the numerical OIDs, text OIDs and actual values of all trap bindings.

---

### 5.10.3 ARP Daemon

The ARP daemon component listens to all network traffic on one or more interfaces and offers the following functionality:

- Collects statistics about MAC addresses being used on the network
- Issues alerts when new MAC addresses are found
- Issues alerts when IP - MAC address mappings are changed

The ARP daemon goes through an initial learning period of 2 weeks after which it assumes to have a useful baseline of all network devices on the network and will alert on new MAC addresses found (if enabled).

The ARP Daemon requires a WinPcap compatible driver in order to capture network traffic. Npcap is currently the driver of choice since the original WinPcap driver is no longer under active development.

**IMPORTANT:** When installing, make sure that "Install Npcap in WinPcap API-compatible Mode" is checked.

---

### Features

**Statistics**

Provides real-time information on MAC address usage and changes.

- When was a MAC address first and last seen on the network?
- With which IP address is a MAC address associated with?
- With which hostname is a MAC address associated with?
- With which vendor is a MAC address associated with?

**Alerts**

In addition to providing statistical information about the network, the ARP daemon also issues alerts under the following circumstances:

- A new MAC address was discovered outside the initial learning period
A MAC address is registering itself with an IP address that is already registered with a different MAC address (possible ARP spoof attempt)

**Setup**

**General**
In order for the ARP daemon component to run, either "Detect new MAC addresses" or "Detect spoof attempts" needs to be checked.

**Interfaces**
Configure on which interface(s) the ARP daemon should listen for network traffic by specifying on or more MAC addresses. While not absolutely necessary, best results are achieved if the interface(s) the ARP daemon is listening is connected to a switch port which receives all network traffic of the switch. A port on the switch which receives all network traffic (as opposed to the default, where it only receives traffic directed to the registered MAC addresses) is usually referred to as a **monitor port**.

---

**5.10.3.1 Event Log & Database**

**Event Log**
When enabled, logs alerts to the event log when a new MAC address is found or when an ARP spoofing attempt is detected.

It is recommended to log ARP spoofing attempts as Errors, especially in security sensitive environments. See "Spoof Detection" for more configurations options and ways to exclude false positives.

**Database**
Configure one or more database which will store the MAC address history as well as current MAC address status.
5.10.3.2 Spoof Detection

ARP spoof detect can alert you when a device on the network attempts to silently redirect traffic away from a legitimate host (usually a router) to an illegitimate host, usually for the purpose of capturing confidential information or disrupting normal operations. See ARP spoofing for more information.

Some legitimate network traffic can appear to be an ARP Spoofing attempt, as such it is important to customize this feature to avoid false positives.

**White-Listed MAC Addresses**
MAC addresses of legitimate network devices such as routers and gateways should be white-listed as they usually associate their MAC addresses with non-local IP addresses. It's also recommended to white-list the MAC address of any other network device that causes false alerts on a regular basis.

**Authorized IP Ranges**
Hosts with dynamic IP addresses (DHCP) can often cause false positives. As such, all IP ranges used by DHCP servers should be added to the “Authorized IP Ranges” list to avoid false positives. This is generally not a security concern since gateways and servers usually do not have IP addresses assigned via DHCP.
You can tweak spoof detection settings here by white-listing certain MAC addresses, or excluding entire IP ranges.

**White-Listed MAC Addresses**
Specify white-listed MAC addresses. White-listed MAC addresses will not generate alerts.

MAC Addresses
00-1D-09-B4-5F-32

**Authorized IP Ranges**
Specify network ranges of IP addresses for which spoof alerts should not be issued, e.g. IP addresses issued by DHCP servers.

Network
195.154.9.193/26
5.10.4 NetFlow

EventSentry can parse the following flow protocols:

- NetFlow v1
- NetFlow v5
- NetFlow v9
- IPFIX
- sFlow

NetFlow monitoring supports the following functionality:

- Visualization, including geolocation, of all network communication sent through NetFlow
- Real-time alerts for traffic to/from certain IP ranges, countries, states, cities, zip codes or city
- Correlation with network logon data to associate network traffic with user names (requires monitoring workstations with EventSentry)

NetFlow is a separately licensed component which requires a NetFlow license. NetFlow functionality is available during an evaluation (where NetFlow functionality is automatically enabled) or when at least one NetFlow license is installed.

To activate the NetFlow collector, check the **Enable NetFlow Collector** check box on the "General" tab and configure either the **database** or **event log** feature. The default NetFlow port is 2055, the default sFlow port is 6343. Both can be changed to another port if necessary. After enabling the NetFlow Collector, you can configure your NetFlow devices to forward data to the EventSentry server on the configured NetFlow ports.

**Aggregate Flows**
To conserve disk space in the database, the NetFlow collector can group multiple flows which are received in close succession of each other. Individual packet details may be lost when this option is activated, but database space is significantly reduced.

**Calculate Bandwidth**
Determines the bandwidth usage of an interface and offers additional metrics compared to traditional SNMP-based bandwidth monitoring. The bandwidth interval determines how often bandwidth statistics are stored in the database.

- Utilization (in %)
- Bytes
- Packets
• Bytes per Packet

Utilization
Calculating the utilization of an interface requires that the NetFlow component knows the maximum speed of an interface, which it tries to determine automatically via SNMP. The maximum speed of an interface can also be specified using variables if the interface speed cannot be determined, or if the maximum speed of the interface does not reflect the actual available bandwidth (e.g. a router has a 1Gb interface but only 100MBit available). Speeds are set in MBit.

Bandwidth utilization that is less than 0.0001% will always be logged as 0.0001%. If the bandwidth utilization cannot be calculated then a 0% utilization will be logged.

The following variables are supported:

• NFSPEED
• NFSPEED[INTERFACENAME]

In order to set a variable, the NetFlow exporter needs to first be added to a group in the management console, and required SNMP authentication credentials need to be set. Once access to the NetFlow exporter is confirmed (Groups -> Check Status), a variable can be assigned by selecting the NetFlow exporter and clicking "Set Variables" in the ribbon.

The device sending NetFlow data will need to be added to a group in the management console before a variable can be assigned to it. The IP address of the device should be added if reverse lookup is not available in DNS.

To add a new variable, click the Add button and specify both a variable name and value. If the speed is set via the NFSPEED variable, then the configured speed will be applied to any interface on the NetFlow exporter. To set the speed for a specific interface, the interface needs to be appended to the variable name. E.g., to set the maximum available bandwidth of the eth0 interface to 100MBit, the NFSPEEDETH0 variable can be set to 100. Interface names are usually displayed on the host inventory page in the web reports.
Assigning a custom interface speed

The NetFlow component will log the following events under the **Network Services** event source during start-up to confirm which interface speeds will be effective:

1005: The interface speed was determined via SNMP
1006: The interface speed was determined via a variable
1007: The interface could not be determined via SNMP and was not set with a variable, bandwidth utilization cannot be calculated at this time

**Bytes**
Stores the number of bytes that were sent and received by the interface during the collection interval.

**Packets**
Stores the number of packets that were sent and received by the interface during the collection interval.

**Bytes per Packet**
Calculates the average packet size during the collection interval.

Monitoring the average packet size can be useful to identify unusual activity on a network, e.g. if the average size is unusually high or low.
**Authorized IP Addresses / Networks**

For enhanced security you will have to specify from which hosts the NetFlow collector will accept packets. Host names are not allowed in this list, only IP addresses may be specified; the CIDR notation is supported.

### 5.10.4.1 Database Consolidation

To consolidate NetFlow data in a database, click the "NetFlow to Database" tab and add one or more databases to the list of databases by clicking the "Add" button.

#### Settings

By default, all received NetFlow data will be sent to the specified database(s). To change this behavior, you can either exclude certain data from being added to the database (include all, exclude some), or only send specific NetFlow data to the database.

Rules can evaluate based on:

- The protocol
• The IP address
• Geolocation (country, state, city, zip code)

Include: Log all NetFlow data to the database, except for exclusions below
This is the default setting and will store all NetFlow data in the database. NetFlow data listed under “Exclusions” will be excluded from processing. For example, traffic to/from certain IP addresses or geolocations can be excluded.

Exclude: Only log specific NetFlow data to the database
This setting is more restrictive and will only store NetFlow data in the database which matches the rules listed under “Inclusions”.

5.10.4.2 NetFlow to Event Log
To log NetFlow data to the event log, click the "NetFlow to Event Log" tab, check the "Log to the APPLICATION Event Log" check box and specify the severity under which NetFlow data should be logged. To avoid flooding the Application event log with NetFlow-related alerts, the frequency of NetFlow alerts can be limited.

Alert Logic
Contains the rules under which NetFlow traffic information should be logged to the event log. Rules can evaluate based on:

• The protocol
• The IP address
• Geolocation (country, state, city, zip code)

Alert on suspicious IP addresses
Logs event 820 (EventSentry Network Services / NetFlow) to the event log if a suspicious IP address has been encountered. The alert includes the source and destination IP address, affected port, threat count and threat details.

**Only if more than ...**
Logs event 830 (EventSentry Network Services / NetFlow) when more than the specified number of bytes are transferred to/from a suspicious IP address within the specified time interval. This can potentially detect irregular network activity such as APTs and also help reduce potential false alarms. Enabling this feature will no longer log event id 820.

**Detect TCP Port Scans**
Logs event 801 (EventSentry Network Services / NetFlow) to the event log if a potential port scan was detected:

- **# of ports:** The number of different ports a remote host has to attempt to connect to in order to trigger an alert (default is 250)
- **Time Interval:** The time interval (in seconds) during which the port scan has to occur (default are 900 seconds)
- **Max Bytes:** Network packets will need to be smaller or equal than this size to be considered part of a potential port scan (default is 250)

### 5.11 ADMonitor

The optionally licensed ADMonitor component monitors changes to all Active Directory objects down to the attribute level (e.g. user accounts, computer accounts, group policy objects) regardless of the current audit settings in a Windows domain.

The ADMonitor component does not have to be installed on a domain controller and has the following advantages over native event log monitoring:

1. Works regardless of current audit settings
2. Detects changes to group policy
3. Shows changes of any attribute change
4. Shows before and after values of attributes
5. Shows who made the change
6. Significantly less storage requirement than capturing all directory service events (event log)
7. Can send out password expiration emails directly to the end user

In addition to capturing AD and Group Policy changes, ADMonitor also provides a current list of all user objects that support queries to isolate users with expired passwords, users who are administrators and more:

- Administrator?
- Disabled?
- Is password set to never expire?
- Is the password expired?
- Does password have to be changed?
- Is the user locked out?
- When was the user created?
- When did the user last login?

In order to determine the last AD logon of a user, the ADMonitor Users pages utilizes either the `lastLogonTimestamp` or `msDS-LastSuccessfulInteractiveLogonTime` Active Directory timestamp, whichever is more recent.
Please note that \texttt{msDS-LastSuccessfulInteractiveLogonTime} is generally more accurate but requires a \texttt{GPO setting} that will display a popup every time a user logs on.

\textbf{ADMonitor vs Account Management Tracking}

For EventSentry users already utilizing the \texttt{account management} tracking feature in \texttt{Security & Compliance}, ADMonitor provides additional details on changes made to Active Directory objects, such as before and after values of attributes.

Since the ADMonitor component only monitors changes to Active Directory (domain users etc), utilizing the account management tracking feature in EventSentry is still recommended for member servers and workstations to detect user and group changes made to the local security database.

\section*{5.11.1 Installation}

The ADMonitor component is installed by the \texttt{configuration assistant} which is automatically run during the installation and/or upgrade of EventSentry. To add the ADMonitor component after EventSentry is already installed, launch the configuration assistant from the start menu.

The ADMonitor component consists of the following:

- EventSentry ADMonitor service
- EventSentryADMonitor domain account
- \texttt{C:\Program Files (x86)\EventSentry\ADMonitor} files

\textbf{Service Account EventSentryADMonitor / Manual Setup}

The EventSentry configuration assistant automatically creates the \texttt{EventSentryADMonitor} service account in the domain during installation; this account is required for the ADMonitor component to work correctly.

Since the \texttt{EventSentryADMonitor} user requires Domain and Enterprise Admin permissions, the user running the EventSentry installation needs to be part of the Domain Admins group; otherwise the user will need to be created by a domain administrator.

To create the \texttt{EventSentryADMonitor} user manually follow the instructions below:

1. Open Active Directory Users and Computers and create a user named \texttt{EventSentryADMonitor}.
2. Add the \texttt{EventSentryADMonitor} user account to the \texttt{Domain Admins} and \texttt{Enterprise Admins} group.
3. On the host where EventSentry is installed, open the \texttt{Services} application and locate the \texttt{EventSentry ADMonitor} service.
4. Enter the properties of the service and set the service account on the \texttt{Log On} tab to the \texttt{EventSentryADMonitor} service. Restart the service.

\section*{Uninstallation}

ADMonitor is removed automatically as part of the EventSentry uninstallation process. The instructions below outline how to only uninstall the ADMonitor component:

- In the ADMonitor dialog in the management console, click uninstall
- Delete the ADMonitor sub directory from the EventSentry installation folder (e.g. \texttt{C:\Program Files (x86)\EventSentry\ADMonitor})
5.11.2 Configuration

The ADMonitor component requires very little customization and automatically configures itself during installation by doing the following:

- Monitors the domain of which the computer is a member of
- Finds the nearest domain controller
- Downloads all Active Directory objects as well as the schema to obtain a baseline. The offline AD database is stored in the ADMonitor\DB sub directory.
- Stores all future changes to objects and group policies in the selected or default database action

Basic Configuration

The ADMonitor dialog in the management console supports setting the target database for all AD changes, controlling the service and verifying that the ADMonitor service is working properly.

Enhanced Configuration

The ADMonitor component supports additional configuration options that can be configured using the EventSentry ADMonitor Console application.

5.11.3 Utilities

The EventSentry ADMonitor component includes three utilities that are intended to be used for troubleshooting purposes and if desired functionality is not available through the web reports. For most users the reporting functionality in the web reports is sufficient and recommended.

The names of the three utilities are listed below and can either be launched from the ADMonitor button in the Home category of the ribbon or through the start menu.

**EventSentry ADMonitor Console**

The console supports the following additional functionality not available via the EventSentry management console:

1. Monitors additional domains
2. Setup global filters to ignore certain AD changes
3. Establish immediate notifications of AD changes
4. Manage data files to conserve disk space

**EventSentry ADMonitor Viewer**

The viewer interacts directly with the internal database and lets users review all AD changes without the EventSentry web reports.

**EventSentry ADMonitor Reporting**

Supports the creation and scheduling of reports for data that may not be available from the EventSentry web reports, for example a list of all organizational units in a domain.

5.11.3.1 ADMonitor Console

The console application lets users configure the following:

- Toggle the monitoring of sub or parent domains
- Filter AD changes deemed noise
- Setup alerts
- Manage data files

**Monitoring Service**
Shows the status of the EventSentry ADMonitor service along with the user account the service is running under

**Set WHO Search Mode**
ADMonitor supports multiple methods to determine who made a change to an AD object, this is configurable in the **Set WHO Search Mode** dialog.
The Enable Detection of "WHO made a change to an Active Directory object" simply toggles recommended default settings, the check box itself is not tied to any actual setting. Settings are controlled via the 3 child check boxes below:

**Analyze "Account Management" events from the security event log**
Utilizes events from the security event log with the "Account Management" category.

**Analyze "Directory Service Access" events from the security event log**
Utilizes events from the security event log with the "Directory Service Access" category.

**Analyze "Directory Services" event log**
Utilizes events from the "Directory Services" event log (only available on domain controllers) which requires additional diagnostic logging to be enabled in this event log; ADMonitor automatically activates this. The volume of additional events logged depends on the network, installed 3rd party software and user activity. This is the most accurate way to determine WHO made a change to an object.

> Activating this setting will enable additional logging under HKLM\System\CurrentControlSet\Services\NTDS\Diagnostics which will affect the volume of events generated in the directory services event log.

**Monitoring Status / Monitoring additional domains**
Additional domains can be monitored if the host where ADMonitor is installed on is part of a domain that has parent or child domains. By default, only the domain of which the computer where ADMonitor is running on is being monitored. Additional domains are displayed in the Monitoring Status area but not monitored by default. Monitoring of additional domains can be activated by double-clicking the domain and checking the "Monitor subdomain.maindomain.com" check box.

**Global Filters**
By default all changes to AD attributes and objects are recorded. To suppress noise the global filter can be used to filter out certain changes, for example changes made to specific objects or attributes. For example, by default changes to the `lastLogonTimestamp` and `msDS-LastSuccessfulInteractiveLogonTime` attributes are ignored by default to reduce noise in the AD change history.

Filters can be configured by clicking the Filter button.
Managing Data Files
Since ADMonitor stores all changes to AD objects in the local cache it may be necessary to either:

- Delete old files
- Compress old files
- Move files to a different location (local or network share)

Regardless of the selected option, data file management always runs at 2:30am.

Checking the "Share for remote Viewer access" check box will share the local DB sub directory as EventSentryADMonitorDB$ (a hidden share) with read access to Domain Admins. This share is utilized by the ADMonitor Viewer to access archived data files remotely. Consequently, this action should be performed on the host where the data files are located. Clearing the check box will remove the share again.

When choosing Network Storage, the target share needs to permit write access to the EventSentryADMonitor user. For enhanced security it's highly recommended to only permit write access to the directory (write-only permission on shares is not supported) as shown in the screen shot below.

Notifications
The recommended way to review changes to AD objects is via the web reports which support on-demand searches as well as scheduled reports. For cases where immediate alerts to AD objects are required, notifications can be setup in the console on the Notifications tab.

5.11.3.1.1 Global Monitoring Filters

Global Monitoring Filters can be used to filter out certain changes to objects that do not need to be audited. Changes that are filtered through a global filter are still recorded in the local ADMonitor Cache, but will not show up in ADMonitor Viewer or web reports.

The table below lists the types of triggers and criteria that can be used to filter changes. Note that multiple conditions can be combined, for example an object change can be combined with an attribute change.

<table>
<thead>
<tr>
<th>Trigger Options</th>
<th>Search What</th>
<th>Description</th>
<th>Search Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Search What</td>
<td>Filter out general changes to objects, usually combined with additional conditions.</td>
<td>was created</td>
</tr>
<tr>
<td>Attribute</td>
<td>Search What</td>
<td>Filter out changes to attributes, such as attribute values or attribute names.</td>
<td>is equal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Principal</th>
<th>Access</th>
<th>Inherited from</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>EventSentryADMonitor</td>
<td>Write</td>
<td>None</td>
<td>This folder, subfolders and files</td>
</tr>
</tbody>
</table>
BIT is set
BIT is not set
was created, modified or deleted
was created
was modified
was rewritten
was created or modified
was created or rewritten
was modified or rewritten
is found
is not found
is equal
is not equal
contains
does not contain

Classname Filter out changes based on the class name.

Object-Name Filter out changes based on the object name.

Object-GUID Filter out changes based on the object GUID.

Who Filter out changes based on who performed the change.

Organizational Unit Filter out changes based on the organizational unit where the change occurred.

Managing Filters

Global Monitoring Filter Settings
Existing filters are displayed in the "Global Monitoring Filter Settings" dialog (1 below), and are managed via the Add, Edit and Delete buttons. Adding or editing an existing filters brings up the Filter Trigger Settings dialog (2 below), which shows the trigger name, description and trigger list.

Filter Trigger Settings
Triggers themselves are listed under Trigger detail (2) and managed via the Edit, Insert and Delete buttons. Inserting or editing an existing trigger brings up the Trigger Line Details dialog (3) where the trigger is configured.

Trigger Line Details
The table above shows the possible trigger options supported, multiple items in the "Search For" list (4) are logically ORed.
In most cases the **Viewer** utility can be used to test a filter and ensure it works as expected.

### 5.11.3.2 ADMonitor Viewer

The ADMonitor Viewer application offers an additional method to view AD changes without requiring the web reports. The ADMonitor Viewer directly accesses the local AD cache and lets users view all AD changes that occurred since ADMonitor was installed. Note that the Viewer **does not** show the following:

- Changes made to Group Policies (requires web reports)
- List of objects like users and/or groups (requires ADMonitor Reporting or web reports)

Results can also be printed and exported in HTML and CSV format.

**Connecting**

The Viewer can either connect to the local ADMonitor cache (default) or to a remote archive if data file management has been enabled. Accessing a remote archive requires that the `EventSentryADMonitorDB$` is available and that the currently logged on user is part of the **Domain Admins** group.

**Searching**

After a connection has been established the search dialog allows the user to specify which change events to display. By default, all object changes from the last 24 hours from all domains are returned. Commonly used search criteria can be saved as a template. Searches can be restricted by:

- Change Type
- Object Name
- Object Class
• User who performed change
• Domain

Advanced searches evaluating the attributes of an object are available as well.

**Sorting / Grouping Results**
Search results are sorted by their timestamp by default, but a custom sort order can be applied by dragging one of the available columns into the dark gray header area. Search/group conditions can be removed by dragging the field outside of the gray header.

**Interpreting Results**
Search results are shown in the main Viewer dialog which is divided into the three sections:

• Object Changes
• Attribute Change Events
• Object Details
Additionally, the Attribute Advisor window (can be toggled) can show a description and details when an attribute is selected.

Object Changes (1)
Shows a list of objects that were changed during the selected search period including the change type, object DN, name, class and timestamps.

Attribute Change Events (2)
All attributes that were modified as part of an object change are shown in this pane since object changes usually consist of one or more attribute changes. Attribute changes include the attribute name and change type, current & previous values including version numbers as well as timestamps. If the attribute advisor dialog is visible then a description of an attribute will be shown when available.

Object Details (3)
Shows all attributes associated with the selected object, such as objectClass, displayName, name and others.

5.11.3.3 ADMonitor Reporting

Active Directory and Group Policy changes along with a current user status list are provided through the EventSentry web reports, the recommended method for ADMonitor reporting.

The ADMonitor reporting application supports a number of scheduled and on-demand reports that may not be available through the EventSentry web reports. The ADMonitor Reporting application provides reports such as:

- A list of all computers, groups or organizational units
- A list of users that have never logged on
- A list of users that have logon or workstation hour restrictions

Reports are divided into either Object Status or Object Change reports and can be scheduled to run at a certain time of the day. Reports are always generated in HTML format.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Run On-Demand?</th>
<th>Schedule?</th>
<th>Create &amp; Customize</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Change</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Object Status</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Reports - Object Changes

The reporting application includes a number of out of the box reports and additional reports can be created with the New button. Object Change reports cannot be run on-demand, they can only be scheduled with a Daily, Weekly or Monthly schedule.

Built-In reports that ship with EventSentry, cannot be modified. To customize an existing report, create a new report - using a built-in report as a template - and then customize the new report instead. Reports created by users are easily distinguishable through a different report icon that includes a user symbol - see screenshot below.

Reports - Object Status
Object status reports only support pre-defined reports and can be run by selecting a report and clicking the Generate (1) button. Generated reports show up in the Generated Reports - Object Status (2) section.

Generating object status reports on demand

**Schedules**
- **Daily**
  Contain AD changes from the previous calendar day.

- **Weekly**
  Contain AD changes from the previous calendar week (Mon - Sun).

- **Monthly**
  Contain AD changes from the previous calendar month (1st - 28/29/30/31th).

It's important to note that the time range for Weekly & Monthly schedules always applies to a calendar day/week/month and **not** the previous 7 or 28/29/30/31 days. A monthly report that is triggered on April 18th will always include data from the month of March.

**6 Web Reports**

The web-based reporting, aka “EventSentry Web Reports, provide the reporting capabilities of EventSentry by making all data collected & consolidated visually available. The web reports can either be installed as part of the main EventSentry setup, or separately with a stand-alone installer.

The web reports can be installed on host on the network as long as it has direct network access to the database server. The following platforms are supported for the java-based web reports:

- Windows
- Linux
- Mac OSX
The web reports installer can be downloaded from the customer area, a live demo is available at https://demo.eventsentry.com.

The Java-based web reports replace the IIS-based web reports from earlier versions of EventSentry and introduce a variety of new functionality including jobs, more granular searching syntax and improved reporting options.

Languages
Support for multiple languages, including German & Spanish, is available in the web reports. Please contact us at support@netikus.net if you would like contribute a translation in your language.

Browser Support
The web reports work with most modern browsers, see requirements for more information. Mobile devices on the iOS and Android platforms are also fully supported.

The web reports do not require any browser plug-ins on the clients (e.g. Java, Flash or Silverlight).

Access Control
Access to the web reports can be restricted so that only users with valid credentials can access the web-based reporting. Users and groups are always created within the web reports, but authentication can optionally be deferred to a LDAP server. Access control lets users be restricted to certain features (e.g. restrict a user to performance reports) or restricted to only view data from certain computers (e.g. restrict a user to only view logs from non-classified servers).

SSL/TLS Support
Web traffic to and from the web reports can be encrypted using SSL / TLS by following instructions in KB article 371.

Java
The web reports require Java 8 (only on the server where the web reports are installed). EventSentry automatically installs and maintains Java as part of its update / patch cycles, its Java installation is not accessible to other applications on the server.

6.1 Pages
The majority of pages in the web reports share 4 common page types which are explained in the sub chapters:

- Dashboard (Network Dashboard, Computer Dashboard)
- Summary
- Details
- Trends

All other page types are unique, including the Network Status, Health Matrix, User / IP Search Pages, Reports, Maintenance Wizard and others.

Page Options
All standard search pages have the option to

- be saved as a report
- be automatically refreshed
show reports for that page type

To access the page option, click the button with three white lines on the top right of the page as shown below.

6.1.1 Dashboard Pages

The Network and Computer dashboard pages are customizable views of one or more tiles showing recent logs entries, trends, system health statuses and more. The network status and health matrix dashboards are discussed separately:

- Network Status
- Health Matrix

Multiple Dashboards
The Network Dashboard supports multiple dashboards which can be shared between users and iterated between.
TV Mode: Click the TV mode button to put the dashboard into full-screen mode. Screen real estate can be further maximized by utilizing the web browser's full screen mode. Please note that iterating through multiple dashboards will exit out of a web browser's full screen mode.

Creating a new dashboard: To add a new dashboard, click the [Change] link on the top left of the screen and selecting Edit. In the resulting screen specify a name for the new dashboard in the “Name” field and click Create.

Sharing a dashboard: A dashboard can be shared by checking the “Public” check box. This dashboard will then appear in the list of dashboards for all others users. Dashboards already shared by other users will appear in the list without the “edit” and “delete” buttons.

Iteration: Instead of displaying only one dashboard, the dashboard page can automatically iterate between all available dashboards every X minutes. Check the “Iterate every” check box and configure a time interval. TV Mode is not available on most platforms while iteration is enabled.

Editing Dashboards: Dashboards can be renamed with the “Edit” button next to the trashcan, dashboards can be deleted by clicking the “Trashcan” button.

Tiles
The network and computer dashboards distinguish between the following tile types:

- Status
- History
- Gauges
- NetFlow
- ADMonitor
Status Tiles
Display the current status of a specific metric, e.g. the heartbeat status or a performance counter. Most status tiles display “OK” when no issues have identified, or the list of warnings and/or errors.

History Tiles
Displays recent changes/events about a monitored metric, such as the most recent service status changes.

Gauges
Display the current status of performance, disk space or environment sensor value. Gauges are only available on the network dashboard.

See tile types for more information.

Layout
The layout can be customized by specifying the number of columns (2 - 4) and the location of the full-width tile (top or bottom). The full-width tile can optionally be disabled as well, useful if you are not utilizing a full-width tile. The screenshot below shows some of the available layout options.

6.1.1.1 Tile Types

Status
Status tiles are available for the following features / metrics:

- Heartbeat Status
- Disk Space Alerts
- Performance (highest & lowest values)
- Process Performance
- Services
- Warranty Information
- Managed Hardware

History
History tiles are available for the following features / metrics:

- Most Active Machines
- Heartbeat History
- Trends (Audit Failures, Error, Syslog)
- Events
- Software Changes
- Generic Search

Gauges
Gauges are available on the network status dashboard, and help visualize performance, disk space or environment data. The following gauges are available:
Heat Maps
Visualize performance data and log volume over the last 24 hours in a unique way, where the x axis shows every available host, and y axis 24 data points, one for every hour. The scale (displayed on the right) of the chart is dynamic, ranging from the lowest value observed to the highest value observed. The heat map makes it extremely easy to spot anomalies of performance and log data from a group of hosts. Unlike trend charts, heat maps visualizes large volumes of data - even across a large number of hosts - very well.

NetFlow
Includes tiles that visualize NetFlow data, including:

- Threats
- Maps
- Trends
- Network Traffic
- Top Hosts (Top Talkers)
- Bandwidth
- Top Ports

ADMonitor
Includes tiles that summarize Active Directory data, including:

- Statistics
- Changes by user
- Changes by computer
- Group Policy changes

Tile Management
Dashboards support single-width and full-width tiles, and individual tiles can be placed freely on the page. Full-width tiles will need to be placed in the full-width area however, which is configured through the "Layout" option.
Tiles are added by clicking the "Add" button on the lower left corner, a tile can be removed by clicking the "X" button on the top right corner of the tile. Tiles can be minimized by clicking the "dash" icon in the menu bar, and refreshed by clicking the double-arrow symbol.

All tiles are available for the network dashboard, but only a small subset of tiles are available for the computer dashboard.

Moving Tiles
A tile can be moved by dragging it with the mouse to a new location until a gray background becomes visible. The gray background indicates where the new location of the tile is going to be. In the screenshot below, the "Automatic Services" tile is moved below the "Disk Alerts" tile where the gray background is visible.

Customizing Tiles
Tiles, once added to the dashboard, can be customized by clicking on the leftmost gear icon in the menu bar. Most tiles allow customization of the automatic refresh interval, the computer from which the data should be obtained, and tile-specific settings. The screenshot below shows a performance tile and its configuration.
6.1.1.2 Network Status

The network status page provides an overview of the overall health status of all monitored servers and workstations on your network using little screen real estate. By default, the network status page shows the current value of 3 key performance counters (CPU, memory and disk usage), but can be customized to show the current status of additional performance counters as well.

Some columns are click-able and will transfer to a different page (e.g. clicking "Computer" will transfer to the "Computer Dashboard") when clicked.
Fields
Heartbeat: Response time of the remote host in ms, or “ERROR” if host is offline.
Services: Shows OK if all services configured for automatic startup are running, otherwise shows the number of stopped services.
Logon: This value shows how many users are currently logged on to the machine.
Software: This value shows the number of applications or patches installed today.

Customization
Clicking “Show Warnings Only” will only show hosts where at least one monitored component is in a warning or error state.

Clicking “Configure” will bring up the configuration dialog, allowing the customization of existing performance counters as well as the addition of new performance counters.

6.1.1.3 Health Matrix
The Health Matrix is a new and unique way to display the health of a large network, while at the same time using as little screen real estate as possible.
Usage
To view detailed information about a host, simply click the tile and review the details on the left pane. Any items which are currently in a warning state will be displayed in red.

Tile size and shape, error threshold and the refresh intervals can all be configured in the left pane. Error threshold and refresh interval changes need to be confirmed by pressing the "Update" button.

Output can be filtered to a specific group with the "Group" drop-down.

Tile Colors
The overall health status of a monitored host is indicated by the color of its square / rectangle / circle (depending on your configuration). The health of a host is calculated using a point system. Any monitored item (e.g. service, disk space, performance counter) which is in a warning state will incur one point. Hosts with no (0) points will have a green status, whereas hosts with 1 point (configurable) will have an orange (warning) status. Hosts with 2 or more (configurable) points will have be in an Error state, with a red color.

<table>
<thead>
<tr>
<th>Status</th>
<th>Points</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td>0</td>
<td>All monitored components are OK</td>
</tr>
<tr>
<td><img src="image2.png" alt="Image" /></td>
<td>1</td>
<td>One monitored component is NOT OK</td>
</tr>
<tr>
<td><img src="image3.png" alt="Image" /></td>
<td>2+</td>
<td>More than one component is NOT OK</td>
</tr>
</tbody>
</table>

Description is based on the default error threshold of "2"

Icons
Both the icon / tile shape as well as size used for hosts are configurable. You can choose between a rectangle, square, a square with rounded edges and a circle. With the exception of the rectangle shape, all shapes are available in small, medium and large sizes.

The rectangle shape is the only shape which displays the host name within the icon. With all other shapes, the host name is retrieved by hovering over the icon with the mouse.

The icon shape and size can be changed using the controls on the lower left side of the screen. Please note this is a global settings, affect matrix reports.

Examples
6.1.2 Summary & Details

All pages retrieving raw log data (e.g. event log, log files, Syslog, SNMP traps, ...) and EventSentry log data (e.g. software installation history, file checksum history) display data in both a "Summary" and "Details" view.

Both views access the same data but display the data differently. The "Summary" view provides a high-level, categorized overview of the collected data to allow the user to quickly understand the type of data that has been collected in the database. Both views share a common page header which includes the search (query) field and the 24-hour trend graph.

The "Detailed" View gives access to the raw data, allowing for a detailed investigation of the collected log data.

Recommended procedure when investigating log data:

1. Access the "Summary" view of the respective log data
2. Narrow the search down by excluding certain items either by utilizing the "X" button or by creating a query
3. Customize the date/time range as well as output count
4. Switch to the "Detailed View"

Time Range
Use the time selection drop-down to customize the time range of the displayed data, 1 hour by default. Select "Custom Range" if the desired time range is not pre-populated in the list.

Query Language
The EventSentry web reports use the Apache Lucene Query Parser Syntax. You can build basic queries by either excluding items (when in the Summary view) or by clicking the search field with the mouse, selecting a field and specifying a search value. See Query Syntax for more information and examples.
If the query syntax is incomplete or incorrect then the search field will show a read X on the left side, as well as details about the location of the error on the right hand side. The search field will show a green check mark if the query syntax is correct.

24 Hour Trend
The 24-hour trend shows a trend line for the current query over the last 24 hours (regardless of the selected time limit). Clicking on a data point on the trend line will narrow the search down to that hour of the day. Depending on the feature, the trend line will either be a line or a bar chart.

The trend line will always show data from the last 24 hours, regardless of the currently selected time range.

The screen shots below show the summary and detailed view of the same data side-by-side. Both views include the search bar, time period selection and graph.
6.1.2.1 Query Syntax

The EventSentry web reports use the Apache Lucene Query Parser Syntax which uses `field:value` pairs for the core syntax. The examples below illustrate the most common syntax based on examples.

Search for all events from the security event log:

| log:Security | Events from the "Security" event log |

Search for multiple values of the same field by grouping the values inside a parenthesis:

| log:(Application OR System) | Events from either the Application or System event log |

Search multiple fields by combining them with the logical **AND** or **OR** operator:

| log:Application AND source:EventSentry | Events from the Application event log with event source "EventSentry" |

Exclude results by prefacing them with a minus:

| log:Security AND id:(-5447) | Events from the Security event log except events with event id 5447 |

Use the `?` wild card to match any single character, use the `*` wild card to match 0 or more characters:

| log:Security AND category:Process* | Events from the Security event log with any category that starts with "Process" |

Use quotes when searching for text strings that contain one or more spaces:


Omit the field name when searching the default field (e.g. the event message for event log searches):

| *john.johnson* OR *jack.jackson* | Events containing "john.johnson" or "jack.jackson" |

Restrict numerical fields to a range of values with brackets:

| log:Security AND id:[4727 TO 4730] |  |
Events for group changes of global security-enabled groups

name: "Applications*CPU" AND value: [5 TO *]
Performance Status: Lists all processes that have a CPU utilization of 5% or more

6.1.2.2 Summary
All pages returning data in textual form (e.g. event log data, syslog data, SNMP data, file checksum data etc.) provide both a "Summary" and "Details" view of the data. The summary view groups data from all relevant data fields to provide an overview of recent data collected by the currently selected feature.

On pages displaying historical data (opposed to pages showing current data, like "Performance Status") the summary view also provides a time line to visualize the distribution of data over the last 24 hours.

Summary / Detailed
Toggle between summary and detailed view. Any custom query is applied to both views. Clicking the "Last Hour" drop-down changes the time period for the current report.

Export Options
Data can be exported in the CSV (comma separated values), XML and PDF format. Frequently accessed search queries can be saved as reports using the "Save as report" link. Reports can be set as the default view for a page and scheduled with jobs.

Group Headers
Clicking on any group header switches to the "group output" page which will display a pie or stacked bar chart.

Including Items
Clicking on an item will update the query and reload the page so that only records matching that item will be returned.

Excluding Items
When hovering over an item in the summary view, a little X will appear next to the text. Clicking on the "X" will refresh the page and exclude this item.

The bottom right shows the load time of the page.
6.1.2.3 Details

Pagination
Output on the detailed view is paginated where up to 500 records can be displayed on a single page. If more records than can fit on a single page are available, a "Next" (and "Previous" button on pages 2 and higher) button will be displayed. The total number of pages is not available since only one result set at the time is being retrieved from the database.

Customizing Output
The visibility of columns can be toggled with the "Columns" button, clicking "Save" will retain the column selection for all future searches of that page. Output can be sorted by any available field in ascending or descending order.

Viewing Record Details
When available, record details can be expanded by clicking the blue double-arrow button as shown below. When viewing event log data, event log record details can also be viewed by clicking on the double window icon.

Export Options
Data can either be exported for the current page (as available on top left), or for the entire (non-visible) result set. Data can be exported in CSV, XML, JSON, RSS and PDF format (PDF format is only available for the current page).
6.1.3 Trends

Visual trends visualize numerical data from the following features:

- Performance
- Diskspace
- Environment (Temperature + Humidity)
- Ping Response
- NetFlow Bandwidth

All trend pages can be exported to PDF format.

Host Name & Feature Selection
All trend pages show the host name selection on the top left, with advanced configuration options specific to the feature right below it.

Time / Date Range
The time / date range for the trend is selected on the top right and ranges from “15 minutes” to “Last Year”. Select “Summary” to view three combined charts for the

- Last 12 hours
- Last 2 days
- Last week

A custom range can be chosen with the “Custom Range” option.

Chart Accuracy
The accuracy of the chart, provided enough data is available, can be controlled with the “Minute | Hour | Day” buttons:

- Day (least accurate, fastest load time)
- Hour (accurate, average load time)
- Minute (most accurate, longest load time)

"Hour" is a sensible choice for most charts, except for charts covering more than one month. "Minute" is only recommended for short time ranges of approximately a day.
6.1.3.1 Feature Specific Trend Pages

Environment

All available sensors (Temperature, Humidity or both) are shown below the host name, including their most current readings.

The unit of measurement for temperature can be switched between Fahrenheit and Celsius.

Disk Space

All monitored drives are shown below the host name, including the volume name, percentage of disk space used and the total disk space of the volume on the right hand side.

The charts can be configured to:

- Show used space or free space available
- Display percent or size

Dynamic vs Static

"Static" will show the full range on the Y axis (e.g. 0 - 100% when choosing "Percent"), whereas "Dynamic" will dynamically scale the Y axis based on the data shown in the chart.
Performance

All performance counters available on the selected host, including their most recent values, are shown below the host name.

Performance counters with multiple instances can be clicked, which will expand and show all available instances. Instances or counters which are in an alerted state will show in red.

Clicking on “Counter” will switch to the performance-counter centric view, which shows the performance history of one or more computers of a counter in one chart.

NetFlow Bandwidth

Shows the IP address of the NetFlow exporter along with all interfaces for which NetFlow bandwidth information is available.

For each interface the following metrics are available:

- Utilization in percent (only available if NetFlow can determine the interface speed, either manually or via SNMP)
- Bytes
- Packets
- Bytes Per Packet

Total shows the combined number of inbound and outbound bytes. Charts that distinguish between outbound and inbound bytes is only available when supported by the exporter, otherwise Inbound/Outbound charts will be empty.

Network Quality

Select a host to view the ping response time of the select time period.

6.1.4 Inventory

6.1.4.1 Switch

Shows all monitored switches and their associated port to MAC address mappings.

Removing duplicates

When switches are cascaded (which they usually are), some MAC addresses will show up multiple times - both on the up-link as well as on the actual port they are connected to. Up-link ports are usually easily identified by having the most devices associated with it. In the screenshot below, port 23 is an up-link port.
Up-link ports can easily be removed from the result set by clicking the “X” symbol to the left of the port. This can be repeated for all monitored switches, and a default report page can be created which will always omit those entries by default.

Details
The detailed view displays all inventoried switch ports, including host name, IP address, MAC address and MAC address vendor. The IP address and/or host names are only available if this information can be obtained from other sources, such as data reported from the agents, ARP daemon and others.

6.2 Page Features
Some pages exhibit unique features which are described below:

Status - Heartbeat
To view the network availability of one more host, switch to the detailed view and review the Uptime, Downtime, Elapsed Time and Availability columns.

Status - Performance
By default, the detailed view of the performance status page shows the most recently collected value of a performance counter. If the time range is changed from “Current” to a specific time range like “Today”, the average from all observed values over that time period will be calculated instead.

Logs - Delimited Log Files
Delimited log files are associated with a log file definition which needs to be selected in order to map the collected data correctly. Since log file definitions changes can affect output, EventSentry keeps a history of all revisions. To view data which was collected with a revision other than the current, the correct revision will need to be selected. Revisions are counted sequentially, with the first (oldest) revision being revision 1.

Compliance - Processes
The “Duration” column in the detailed view supports the range operator in the query field. For example, `duration:[180 TO *]` will only show processes which ran for 3 minutes or longer.

Compliance - Policy Changes - Audit Policy
On Windows 2003 and earlier, lists all the 9 available policy categories and their effective values for both success and failure. Windows 2008 and later contain significantly more auditing categories than earlier versions of Windows, and as such only the categories whose values have changed are listed. As such, the Subcategory and Subcategory GUID fields contain detailed information about the changed policy.

Compliance - Policy Changes - Trust Relationships
The “SID Filtering” column indicates whether SID Filtering is enabled or not for the trust.

History - Uptime
The uptime history is updated by the agent after a server or workstation is rebooted or powered on. As such, the uptime report will not reflect the current uptime of a host - review the Inventory - Computer page instead.

Inventory - Computer
The computer inventory page shows detailed hardware information about a host, including model & serial numbers, installed memory, controllers and network cards, hard drives and much more. The tabs Software, Processes & Changes are only available on Windows hosts which are monitored with an agent.

**Hardware by DELL or HP**
A warranty field will show when the warranty of a computer has or will expire, including additional information about the type of warranty available for that computer. If the vendor's management software (e.g. DELL OpenManage) is installed, then additional information about server components like power supplies, system fans, temperature sensors and more is available on the **Managed Hardware** tab.

**Non-Windows Hosts monitored via SNMP**
Only the "Hardware" tab is available on hosts monitored through SNMP, and only a subset of the information will be displayed compared to Windows hosts monitored with an agent.

### 6.3 Reports & Jobs
Frequent searches can be saved as reports from almost all pages (with the exception of most pages under “Dashboards” and “Settings”). Reports can also be scheduled to run automatically with jobs.

To create a report, run and customize any page and click the "Save as report“ button. If the “Save as report” button is not available, click the options button on the top right of the page.

When creating a new report, the following fields can be specified:

- **Report Name**
- **Report Category**
- **Description (optional)**
- **Page Default**
- **Create Job**

**Page Default**
Every page in the web reports can have a "Page Default" report associated with it. If a page (e.g. Heartbeat - Status, Trends - Performance) has a default report associated with it, then that report will be loaded (in place of the default “Summary” view) when the page is accessed. As such, there can only be one "Page Default" report per page.

**Editing Reports**
Existing reports can be managed through the "Reports - List Reports" page where one can edit, run, delete and review all configured reports. All properties of a report, with the exception of the page type, can be edited after a report has been created. Only reports associated with the currently active profile or reports configured for "All Profiles" will be listed.

**Review**
If a report needs to be reviewed on a regular basis, then "Require a review" can be configured. Reports that have not been run in the required time period will
appear in the "Overdue Reports" widget on the Network Dashboard as well as on the "List Reports" page. A report can be configured for a review by clicking the "Review" button in the "List Reports" page.

**Built-In Reports**
EventSentry ships with a number of built-in reports which are loaded the first time the "Built-In Reports" tab is clicked. Built-In reports behave like regular reports and can be edited, delete and so forth.

**Profiles**
By default, a report is automatically associated with the current profile, and will only show up in the report listing for that profile. A report can either be associated with a single profile (default) or all profiles.

**Jobs**
When creating or editing a report, a job can immediately be created by checking the "Create Job" check box. Jobs can also be managed on the "Reports - Jobs" page.

Existing reports can be managed through the "Reports - List Reports" page.

**Copying reports to different computers**
Reports from all profiles are stored in the "reports.xml" file, located in the "WebReports\conf" sub directory of the EventSentry installation directory. The XML file can be copied to/from a different host simply by replacing the reports.xml file.

**Report History**
Any time a report is run manually (and not as part of a job), details about the execution of the report are added to the report history. The following information about a report is available in "Reports - Report History":

- Date/Time
- Report Name
- Username
- Load Time
- Returned Results (if applicable)

---

**6.3.1 Jobs**

Jobs automatically run reports on a specific interval and are sent to one or more recipients via email.

Clicking the "Add Job" button on the top right corner of the "Jobs" page will create a report. Like reports, jobs can be edited or deleted on the "Jobs" page with the "Edit" and "Delete" links.
**Format**
Reports can be sent in either a HTML, PDF or CSV format.

**Send Empty Reports**
When set to “Yes”, reports are sent even when they contain no data (if the underlying report does not yield any records). When set to “No”, reports are only emailed when they contain at least one record set.

**Profiles**
If a report is associated with "All Profiles", then the job will need to set the profile under which the report is to be run. If the report is already associated with a specific profile, then the job will also use that profile.

**Email**
Emails sent by a job can be highly customized, by setting the sender email, CC and BCC recipients, subject and message text. The following variables are supported in the subject:

- $FREQUENCY
- $REPORTNAME
- $RECORDS

**Frequency**
Jobs can be sent out once, or at configurable frequencies:

- Minutely
- Hourly
- Daily
- Weekly
- Monthly

### 6.3.1.1 ADMonitor User Password Reminders

Since ADMonitor knows when a user's password expires, it can send out daily password expiration emails directly to the end user when the password is close to expiring. The only requirement is that there is a predictable way to dynamically build the email address of the end user using one of the user attributes available in the web reports.

Password expiration emails are configured in the Reports -> Jobs page in the "Email User Password Expiration Reminders" section. New reminder emails are added with the "Add Reminder" link, and multiple reminder emails can be configured (e.g. to target different domains).

**Remind when expiration (days)**
Sends an email if the password expires within the selected number of days

**Prefer email attribute if available**
AD includes an email attribute. When checked and an email attribute is configured, it will be used first.

**Email Format**
If the email attribute is not set on a user, the email address needs to be built dynamically using the available variables:

```
$UPN
$FIRSTNAME
$LASTNAME
$FIRSTNAME_INITIAL
$LASTNAME_INITIAL
$SAM
```

This feature cannot be used if the email address cannot be defined using the available variables (e.g. using a middle initial).

**Filters**
The password reminder email feature enumerates all active user accounts by default but can be restricted to only apply to a specific domain or only to administrative users.

6.4 **Maintenance**

The maintenance section provides functionality to maintain and manage the EventSentry database.

**Maintenance Wizard**
The maintenance wizard purges old data from the database, see Maintenance Wizard for more information.

**Database Usage**
This page shows how much space is being used in the EventSentry database, broken down by feature. The statistics available for each database may vary. The page is available for the built-in PostgreSQL and Microsoft SQL Server® databases.

**Agent Status**
This page shows the last time an agent on a monitored host wrote data to the database, broken down by the following features:

- Event Log
- Heartbeat
- Performance
- Disk
- Environment

6.4.1 **Maintenance Wizard**
The Maintenance Wizard allows old data to be purged from the EventSentry database. Data can also be purged automatically with a command-line utility.

All data deleted with the maintenance wizard will be permanently removed, and there is no way to get the data back unless you have a working database backup. The Maintenance Wizard will prompt for the database administrator login/password (e.g. postgres, sa, ...) for all tasks.

**General**
Performance Counter: Removes all references to the selected performance counter(s)
Logical Drive: Removes all references to the selected logical drive(s) on the selected host
Binary Data: Removes all binary data
Virtual Machine: Removes virtual machine information
Log File: Removes log file definitions

Hosts
All Instances: Removes all data of the selected host(s)
Certain Instances: Removes one or more instances of the selected host (e.g. remove all event log data only)

- Computers are flagged as "orphaned" by the management console when a computer from an Active Directory-Linked group is removed from Active Directory. Clicking the "Orphaned computers" check box will automatically select all computers which are marked as orphaned.
- When removing all or some instances, only computers running an agent are shown by default. To remove hosts which are not running an agent, click the "Include hosts without an agent" check box. In most cases this will significantly increase the number of hosts shown.

Tuning
Tuning lets you remove data that is older than a certain amount of days from all or selected instances. For example, all File Access and Process Tracking data which is older than 90 days can be removed. Tuning can either be applied to all or just select hosts.

Instead of purging the data immediately, a set of SQL statements can be generated with the SQL button at step 3. The SQL statements can then be run at a later time.

6.4.2 Collector Status
The collector status page provides performance and health statistics of any installed collector. "Collect Statistics" must be enabled in the collector configuration for this page to display information.

Compression Level
The observed compression level.
Connections
The number of agents connected to the collector.

Inbound Queue
The number of packets which have been received by the collector but not yet been decoded for processing. A sustained high number may indicate that the collector does not have enough CPU resources to process packets.

Outbound Queue
The number of data items that have been successfully decoded from the inbound queue but not yet sent to the action. The number of items in the queue should be low, a large outbound queue length usually indicates a performance issue with the database.

Bytes Per Second
The number of bytes per second received.

Packets Per Second
The number of packets per second. Each packet may contain one or more data items (e.g. event log entry, performance data, etc.)

Invalid Packets
A packet is deemed invalid if it cannot be decoded. Invalid packets may occur if there is a (significant) version mismatch between the collector and the agents. This number should always be 0.

6.5 Settings

6.5.1 Profiles
Profiles support multiple database connections within a single installation of the web reports. By default, only one profile is setup. Multiple profiles are useful in a variety of scenarios:

- Switching between a primary and archival database, or between multiple databases
- Switching between databases of different customers ("multi-tenancy")

In general, a profile sets the language, database connection properties as well as the email settings (which are used primarily for jobs).

When Access Control is enabled, users can be restricted to one or more profiles.

You can switch between profiles by clicking the profile name ("EVENTSENTRY" by default) on the top left screen of the web reports as shown below:

Profile Settings
Default Profile
This is the profile which will be loaded by default when multiple profiles are present
UTC
This setting needs to match the setting in the "Global Options" of the management console. When agents write data in the UTC date/time format, the web reports display all timestamps in the local timezone, as configured under Settings.

**Creating and deleting profiles**

*Creating a new profile:* To create a new profile, navigate to "Settings - Profiles" and click on "Create New Profile" on the top left. Specify all required profile settings and click the "Submit" button on the bottom.

*Deleting a profile:* To delete a profile, first switch to the profile you wish to delete by clicking on the profile name on the top left. Then, navigate to "Settings - Profiles" and click the "Delete Current Profile" button.

### 6.5.2 Access Control

Access to the web reports can be restricted so that only authenticated and authorized users have access. Access control also supports multi-tenancy by giving users only access to data from certain hosts.

Access control supports the following:

- Create users and groups
- Authenticate users via LDAP(S)
- Restrict users to a set of areas in the web reports
- Control access to profiles
- Block certain areas in web reports from users
- Restrict users to view only data from specific hosts

The default user name for the first user is "admin" when enabling Access Control as part of the EventSentry installation.

Access Control can be enabled when you first setup EventSentry and the web reports, or at any time after that by navigating to Settings -> Access Control. When enabling Access Control, at least one user will have to be created ("admin" by default).

**LDAP**

By default, user accounts use built-in authentication where the user password is managed by the web reports. If a Windows Active Directory infrastructure is available, then it's recommend to enable LDAP support, so that user do not have to manage multiple passwords. When enabling LDAP support, authentication can be deferred to a LDAP(S) server when creating an account of type "Windows Authentication (LDAP)".

![Add User dialog](image)

To enable LDAP support, switch LDAP Support to "Enabled", click the "Configure LDAP Server" link and specify the IP address or host name of a domain controller running LDAP.

**Managing Users**
Users are added and removed by clicking the respective user icons in the “Users” tab. If LDAP support is enabled, users can either be enabled with Built-In Authentication or with Windows Authentication (see “LDAP” above). When creating users, you can specify:

- User Name
- Full Name
- Password (Built-In Authentication only)
- Email Address (for password recovery, built-in Authentication only)

Managing Groups

Groups are added and removed by clicking the respective group icons in the “Groups” tab. The same privileges and permissions that can be assigned to users can also be assigned to groups.

6.5.2.1 Permissions & Privileges

By default, user accounts and groups have all privileges enabled and have access to all pages, reports and computers.

All information in this chapter applies to both user accounts and groups.

Privileges

The following two privileges are available:

- **Manage Accounts**: Allows a user or group to create, edit and delete users. This should only be assigned to administrators.
- **Manage Profiles**: Allows a user or group to create, edit and delete profiles.

Allow vs Blocked

Pages, reports or computers can either be allowed or blocked. If an item (e.g. "Event Log Search") is added to the Allowed list, then the Allowed list will become active, and the user or group will only be allowed to access pages which are in the Allowed list - the Blocked list is disabled.

If an item is added to the Blocked list, then the Blocked list will become active, and the user or group will only be disallowed to access any pages which are on the Blocked list.

If a user or group should only have access to a limited number of pages, reports or computers, then those items should be added to the respective “Allowed” list. If a user or group should have access to the majority of the web reports, but you wish to block certain pages, reports or computers, then those items should be added to the “Blocked” list.

Pages

Allow or block any page in the web reports. Pages to which the user or group does not have access to (either because it's not allowed or because it's blocked) will not be visible in the menu.

Reports

Allow or block any report in the web reports.

Computers

Allow or block computers from results, this applies to all pages and reports.

User vs. Group Permissions

Permissions, such as allowed pages or blocked pages, are accumulated if a user is a member of multiple groups, or when permissions are assigned on both the user and group level. Blocked features
(e.g. blocked pages, blocked reports or blocked computers) always take precedence over allowed features.

The table below shows how different permissions on a user level and multiple group membership are merged into the effective permissions:

<table>
<thead>
<tr>
<th>Examples</th>
<th>User Permissions</th>
<th>Group 1 Permissions</th>
<th>Group 2 Permissions</th>
<th>Effective Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allowed Pages</td>
<td>Blocked Pages</td>
<td>Allowed Pages</td>
<td>Blocked Pages</td>
</tr>
<tr>
<td>Example #1</td>
<td>Disk Trends</td>
<td>Performance Trends</td>
<td>Syslog Search</td>
<td>Disk Trends</td>
</tr>
<tr>
<td></td>
<td>Disk Status</td>
<td></td>
<td></td>
<td>Disk Status</td>
</tr>
<tr>
<td>Example #2</td>
<td>Event Log Search</td>
<td>Syslog Search</td>
<td>Software Installed</td>
<td>all other</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Software History</td>
<td>Syslog Search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Software Installed</td>
<td>Software History</td>
</tr>
<tr>
<td>Example #3</td>
<td>Computer Dashboard</td>
<td>Maintenance Wizard</td>
<td>Computer Dashboard</td>
<td>all other</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**6.5.3 Preferences**

**Timezone**
When UTC is enabled, configure the time zone in which all timestamps should be displayed in.

**Appearance**
Configure the basic color schema.

Preferences are specific to a user account, unless **Access Control** is disabled, in which case it applies globally.
7 Additional Tips and Resources

This chapter contains additional information not directly related to EventSentry but useful for event log and system monitoring:

Database Tips

- Tuning the EventSentry database
- Purging records periodically
- Encrypting Network Traffic with MSSQL

Event Log Reference

- 1. Windows NT Security Event Descriptions
- 3. Common events from systems in the field

7.1 Database Tips

This chapter contains tips and tricks for all database-related tasks.

- Tuning the EventSentry database
- Purging records periodically (example for MS SQL Server)
- Encrypting Network Traffic with MSSQL

7.1.1 Tuning the EventSentry Database

The EventSentry database is designed to accommodate large amounts of data while still providing fast query responses. When you expect large amounts of data (e.g. more than 1 million records) it is however still important that you take steps to ensure that the database is optimized at all times. Below you will find recommendations for various supported databases when you expect to collect large amounts of data.

Microsoft SQL Server®

1. When creating the database, make sure that you set the initial database size sufficiently high. This will improve the overall performance because the database engine will not have to continuously extend the data files. This applies to both the data files and the transaction log size. In addition, configure the file growth rate larger rather than smaller. The screenshots below show a good starting point for potentially large databases:
2. Reorganize the tables on a regular basis, but especially after you purge or move old records. SQL Server offers a feature called **Maintenance Plan** that lets you schedule a database maintenance on a regular basis or by demand. Keep in mind that a database reorganization can temporarily use more disk space, so always make sure that you have enough disk space for the database and transaction log available. The maintenance plan wizard can be launched by right-clicking the database and choosing "Maintenance Plan" from the "All Tasks" submenu. The screenshot below shows a recommended configuration.
7.1.2 Purging Records

The event log consolidation and process tracking tables might grow too large after a while. You can configure your system to periodically purge records that are no longer relevant, e.g. after 12 months. This chapter shows:

- How to use the included database purge utility to purge records automatically on all supported databases
- How to setup scheduled jobs on Microsoft SQL Server® to automate the purging of records

EventSentry includes a command-line application that can purge records from the EventSentry database. The utility can be scheduled to run on a regular basis using the EventSentry application scheduler or the Windows Task Scheduler. See Purging Records Automatically for more information.

Setting up an automatic job (Microsoft SQL Server® 2005 and later)

1. Open the “Microsoft SQL Server® Management Studio” and navigate to “SQL Server Agent” -> “Jobs”.
2. Right-click “Jobs” and select ”New Job ...
3. Specify a name for the job (e.g. ”EventSentry Database Purge”) and click on ”Steps” in the left pane.
4. In the steps window, click the ”New...” button.
5. Give the step a descriptive name and paste one of the SQL statements below. You can specify multiple SQL statements, but separate them with a `GO` statement in a single line. You can obtain the SQL statements from the last step of the web-based maintenance wizard.

6. Make sure the correct database is selected.
7. Click the "Advanced" tab and select "Go to the next step" for the "On failure action" setting. Click **OK**.
8. Add another step if necessary.
It is recommended that you purge data frequently (with smaller amounts of data affected at each purge) to reduce the impact of the purge on the database. For example, instead of setting up a job to delete records that are older than 180 days once a month, set the job up to run at least once a week. This way each job will affect less data and as such complete more quickly.

9. Click “Schedules” and add a new schedule.
10. Give the schedule a name (e.g. Weekly) and configure the schedule.
11. Click on “Notifications” to enable error reporting. Check the box “Write to the Windows Application event log” and select “When the job completes”. You can change this option and only log an event if the job fails.
12. Click OK to add the schedule

7.1.2.1 Purging Records Automatically

You can automatically purge records from PostgreSQL and MSSQL databases using the es_db_purge.exe command-line application. You can either run this tool at your convenience, or you can automatically schedule it to run on a regular basis (e.g. every Sunday) to completely automate the process of permanently removing old data.

The utility lets you specify which feature you would like to purge (e.g. event log data and performance data) and how many days you would like to keep (e.g. 180 days).

The database purge utility works through ODBC (the same way all other components connect to databases) and can be configured using command-line arguments.

All data purged by this application will be permanently erased and only be accessible when restored from a working backup.

See Database Purge Utility for more information.

7.1.3 Archiving event log records

Consolidating event log records in a central database can be a challenge for database servers that aren't adequately sized, especially in medium and larger networks where the EventSentry database can easily grow to hundreds of gigabytes or even terabytes in size. If the database server is under too much pressure, then certain EventSentry components may start queuing data and search queries in the web reports can take longer to complete.

While EventSentry does not offer a feature to automatically archive events to a separate archival database, EventSentry can be configured to write log data to two databases: One database for fast access (this database purges older records on a regular basis) and another database for long-term archiving. Due to EventSentry's flexibility you can even use two different database types for this task. For example, a Microsoft SQL Server® database can be used to store immediate data (e.g. last 60 days), and a PostgreSQL database can be used to store data for long-term storage (e.g. 2 years).

The following three EventSentry features support this setup:

1. **Filter Rules**: EventSentry's filter rules can forward the same event to multiple notifications, for example to two different databases.
2. **Notifications**: EventSentry allows setting up multiple notifications of the same type, for example multiple databases.
3. **Profiles**: The web reports support multiple profiles so that multiple databases can be accessed from the same URL.

The instructions below assume that a database consolidation is already setup and will walk through the process of setting up a second database for archival purposes.

### 1. Create an action

EventSentry needs an action in order to forward events to a database. In the EventSentry management application, click the "Actions" container in the left tree view. Then, either use the ribbon to add an action or right-click the actions container and select *Add*. Enter a descriptive name for the action, e.g. "Secondary Database" or "Long-Term Database".

In the resulting dialog click the *Initialize or Update Database* button to launch the **Configuration Assistant** in database initialization mode. Simply follow the wizard which will create an initialize the schema on a new database.

> If you are creating the first EventSentry database on a DB server, make sure you document the passwords for both the `eventsentry_svc` and `eventsentry_web` users.

When the configuration assistant is complete, it will automatically configure the database properties for the action. Click the "Test" button to ensure the action configuration is valid.

### 2. Modify or create an additional filter rule

Now that the new database is initialized, events can be forwarded to it. The easiest way to forward events to a 2nd database is to modify the pre-existing filter rule that forwards your events to your primary database.

Edit each filter rule in the Database Consolidation package and add the new notification to the *Actions* list. If you cannot see the list of actions then your actions are inherited from the package-level and you will have to change the package details. Right-click the parent package and select *Edit*. There, add the new action to the *Actions* list of the *Overrides* section.

You can also create an additional filter rule instead of modifying the existing one for better structure. After saving and pushing the configuration, the selected events are being written to both databases.

You can also adjust other features that support multiple databases, including:

- Log File Monitoring
- Performance Monitoring
- Validation Scripts

### 3. Purging records periodically

Once data is written to both databases, a purging schedule needs to be setup based on the following factors:

- How long to keep the records in the fast-access database, for example 60 days.
- How long to keep the records in the archival database. This depends on the compliance or management requirements.
- Which database server to select as the fast-access, and which for the archival database. This is usually an obvious choice.

Once you have determined these factors you can setup both databases up to purge records periodically. Please see [Purging Records](#) and [Purging Records Automatically](#) for more information.

### 4. Creating a new profile in the web reports
Profiles allow you to setup additional database connections and/or interface settings. After an additional profile is created you can simply access it by selecting it from the Drop-down list from the top left. Profiles are created through the Profile Editor or by editing the configuration.xml file directly.

In the web reports menu, click the gear icon, choose Profiles, and click Create New Profile on the left. Assign the profile a descriptive name in the Profile Name section and configure the database connection accordingly. Please also make sure that other settings (e.g. the UTC settings and Email Settings) are configured correctly.

Once you click Submit at the bottom of the page you can simply switch between your primary and secondary database by selecting the pull-down menu from the top left.

7.1.4 Microsoft SQL Server

7.1.4.1 Encrypting Network Traffic with MSSQL

Most ODBC drivers, including Microsoft SQL Server®, transmit network traffic in clear text which can be a problem in security sensitive environments. Microsoft SQL Server® supports protocol encryption which encrypts all traffic between the client (=EventSentry agent) and the Microsoft SQL Server®.

Using protocol encryption requires the following prerequisites:

- Certificate Services installed on machine running in your domain
- Latest SQL Server ODBC drivers installed on all clients (Microsoft® ODBC Driver 13.1 for SQL Server)

This chapter will guide you through the process of setting up Active Directory Certificate Services and requesting a certificate so that SQL server can use protocol encryption. This chapter is based on using Windows Server 2016 for the OS and Microsoft SQL Server® 2016/Microsoft SQL Server® 2019 for the database

1. Installing Certificate Services
   You will only need to follow these steps if you do not have certificate services running in your domain. If you already have a certificate server in your domain then you can skip step 1.

   Navigate to "Start -> Administrative Tools -> Server Manager -> Manage -> Add Roles and Features":

   ![Server Manager](image)

   Which will launch the “Add Roles and Features Wizard” similar to this:
Step-by-step instructions for installing the Active Directory Certificate Services

2. Configuring the MMC snap-in
   In order to manage/create certificates you need to configure an MMC for the certificate services. To open the Certificates snap-in, follow these steps:

   - To open the MMC console, click Start, and then click Run. In the Run dialog box type: mmc
   - On the Console menu, click Add/Remove Snap-in....
   - Click Add, and then click Certificates. Click Add again.
   - You are prompted to open the snap-in for the current user account, the service account, or for the computer account. Select the Computer Account.
   - Select Local computer, and then click Finish.
   - Click Close in the Add Standalone Snap-in dialog box.
   - Click OK in the Add/Remove Snap-in dialog box. Your installed certificates are located in the Certificates folder in the Personal container.

3. Installing a certificate on the server
   In the MMC, click to select the Personal folder in the left-hand pane. Right-click in the right-hand pane, point to All Tasks, and then click Request New Certificate....which will bring up the dialogs shown below:
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate
The **Certificate Request Wizard** dialog box opens. Click Next. Select Computer as the Certificate type.

After the wizard finishes, you will see the certificate in the folder with the fully qualified computer domain name.

4. **Requiring database encryption for all communication**

   Once the certificate is installed you can configure the SQL Server to "Force protocol encryption".

   **• For SQL Server 2016/2019**

   Navigate to “Start -> Microsoft SQL Server 20xx -> SQL Server 20xx Configuration Manager.” Expand "SQL Server Network Configuration". Right click on "Protocols for MSSQLSERVER" and choose Properties. Set "Force Encryption" to "Yes" then click on the Certificate tab where you have to select the certificate you created above.
When not using the collector, all clients communicating with the SQL Server will need an up-to-date SQL Server ODBC driver installed in order to support encryption. If a machine is unable to communicate with the database server after you enabled encryption, installing the latest ODBC driver from Microsoft® ODBC Driver 13.1 for SQL Server will usually resolve the problem.
7.2 Screenshots

7.2.1 Main Configuration Window

![Main Configuration Window](image)

EventSentry 4.0 Beta: Monitor Active Directory in detail with new ADMonitor component

One or more EventSentry crash dumps were found - click here for instructions.

- Step 1: Add hosts to EventSentry (import or link from AD or files, network discovery, manually)
- Step 2: Deploy agent to remote hosts
- Step 3: Access Web Reports

Maintenance agreement is valid until Mon 1/27/2020
7.2.1.1 General Options

The EventSentry service is the core monitoring component of the EventSentry monitoring suite. It allows for real-time monitoring of the event logs, log files, system health components and compliance-related events. You can install the agent on remote servers using Remote Update.

Agent

- Stop
- Restart
- Uninstall

Service Maintenance: Update...
Change Startup Type to: Manual

Version: 4.0.0
Instal Status: Files, Service
Debug Level: Low

Create Test Events

Collector

Stop
Restart

Memory Usage:
CPU Usage:

Heartbeat Monitor

Stop
Restart

Memory Usage:
CPU Usage:

Network Services

Stop
Restart

Memory Usage:
CPU Usage:

ADMonitor

Stop
Restart

Memory Usage:
CPU Usage:

Web Reports

Stop
Restart

Memory Usage:
CPU Usage:

Service Options
General GUI Options

Options

General
- Always minimize to tray
- Automatically collapse unselected groups
- Require double-click to edit objects
- Use ribbon-style toolbar (requires restart)
- Show Features Button in Status Bar

Tray Area Notifications
- Show notifications as: Popup Window
- Show for: 5 seconds
- Sound Notification
- Enable

Automatic Configuration Backup
- Backup daily and keep last 30 backups
- Folder: C:\Program Files (x86)\EventSentry\Backups

Auto-Close (Idle Detection)
- Enable
- Automatically close application after 30 minutes of inactivity
- Behavior with unsaved changes: Skip Auto-Close

[OK] [Cancel] [Help]
7.2.1.2 Welcome Screen

EventSentry 4.0 Beta Monitor Active Directory in detail with new ADMonitor component

One or more EventSentry crash dumps were found - click here for instructions

Step 1: Add hosts to EventSentry (import or link from AD or files, network discovery, manually)

Step 2: Deploy agent to remote hosts

Step 3: Access Web Reports

Maintenance agreement is valid until Mon 1/27/2020

Welcome Screen

- [ ] Display Welcome Screen on Startup
- [ ] Fetch news from https://www.eventsentry.com
7.2.1.3 Environment Monitoring

Temperature / Humidity Sensor | Motion Sensor | Smoke Sensor | Water Sensor

COM Port
Serial Port: COM1 Communications Port

General Settings
Scale & Type: Fahrenheit
USB
Calibrate...

Measure the following:
- Temperature Position: 1
- Humidity Position: 1

Current Measurements
Temperature 76 F
Humidity 21 %

Calibration offsets are not applied

Limits
- Enable Temperature Alerts
- Specify desired range: 60 to 85 degrees
- Enable Humidity Alerts
- Specify desired range: 10 to 70 %

Notify me at most every 6 hour(s)

Database
Record in database: Primary Database every 1 hour(s)

© 2002 - 2022 ... NETIKUS.NET ltd
7.2.1.4 Syslog Configuration Window

![Syslog Configuration Window](image)

- **Syslog Daemons**
  - Syslog UDP, Port: 514
  - Syslog TCP, Port: 514
  - Syslog TLS, Port: 10514

- **Threshold Settings**
  - Limit how many incoming messages will be allowed in a given time period.
  - Maximum number of allowed messages: 40000
  - Time Period: 1 hour

- **Authorized IP Addresses / Networks**
  - 0.0.0.0/0
  - 255.255.255.255/32
  - For enhanced security, you can specify which hosts or networks the daemon will accept packets from. You can also accept messages from any host.
  - Accept messages from all hosts
  - Network
    - 192.168.6.0/24
Additional Tips and Resources

General Syslog Settings  Syslog to Database  Syslog to Event Log

Use this dialog to configure how EventSentry should log syslog messages to a database.

Destination

Databases: Primary Database

Add  Delete

Settings

Include: Log all Syslog messages to the database, except for exclusions below
Exclude: Only log Syslog messages to the database that are included below

Exclusions:

*snbd*

List of lines that are to be included or excluded from incoming syslog messages ...

General Syslog Settings  Syslog to Database  Syslog to Event Log

Use this dialog to configure how EventSentry should log syslog messages to the event log.

Destination

Log to the APPLICATION Event Log

Severity Mapping

<table>
<thead>
<tr>
<th>Unix</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>emerg Error</td>
<td></td>
</tr>
<tr>
<td>alert Error</td>
<td></td>
</tr>
<tr>
<td>crit Error</td>
<td></td>
</tr>
<tr>
<td>err Warning</td>
<td></td>
</tr>
<tr>
<td>warning Warning</td>
<td></td>
</tr>
<tr>
<td>notice Information</td>
<td></td>
</tr>
<tr>
<td>info Information</td>
<td></td>
</tr>
<tr>
<td>debug Ignore</td>
<td></td>
</tr>
</tbody>
</table>

Set Defaults

All incoming syslog messages are logged to the APPLICATION event log with event id 500, using the "EventSentry Network Services" event source.
7.2.1.4.1 Syslog Example Eventlog Record

Event Properties

Event Properties

<table>
<thead>
<tr>
<th>Event</th>
<th>Event Properties</th>
<th>Event Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>2/4/2003</td>
<td>Source: EventSentry</td>
</tr>
<tr>
<td>Time</td>
<td>2:56:43 PM</td>
<td>Category: Syslog</td>
</tr>
<tr>
<td>Type</td>
<td>Information</td>
<td>Event ID: 9999</td>
</tr>
<tr>
<td>User</td>
<td>N/A</td>
<td>Description:</td>
</tr>
<tr>
<td>Computer</td>
<td>BLACKJAGUAR</td>
<td>syslog@netikus-router[crontime]: CROND[5535]: (root) CMD (run-parts /etc/cron.hourly)</td>
</tr>
</tbody>
</table>

Data: Bytes | Words

OK | Cancel | Apply
7.2.1.5 Filters & Actions Configuration Window
7.2.1.5.1 Filter Configuration Window

The Filter Configuration Window allows users to configure settings for filtering and managing event logs. The window is divided into several sections:

**General**
- Actions: Default Email
- Trigger all actions
- Log:
  - Application
  - Directory Service
  - Security
  - File Replication
  - System
  - DNS Server
- Event Severity:
  - Information
  - Critical
  - Warning
  - Error
  - Audit Success
  - Audit Failure

**Filter Settings**
- Include
- Exclude
- Advanced...

**Details**
- Event Source: EventSentry
- Category: Heartbeat Monitoring
- Event ID:
- Username:
- Computer:

**Content Filter & Notes**
- Content Filters:
  - Type: Wildcard
  - Wildcard
  - Wildcard
  - Filtertext: "Testground" "Workstation"
- Chain multiple content filters using a:
- OR (default)
- Notes:

The window provides options to configure various aspects of event filtering, including actions, log types, event severity, and detailed settings for content and notes.
7.2.1.5.2 Action Configuration Window

SMTP Action

<table>
<thead>
<tr>
<th>General</th>
<th>Display &amp; Delivery Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender Name:</td>
<td>HTML (Modern)</td>
</tr>
<tr>
<td>Sender Email:</td>
<td>Customize ...</td>
</tr>
<tr>
<td>Recipients:</td>
<td>Header / Footer</td>
</tr>
<tr>
<td>Subject:</td>
<td>Low</td>
</tr>
<tr>
<td>Importance:</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Flag Literal</td>
</tr>
</tbody>
</table>

Primary Email Server (SMTP)

- Host: 192.168.4.33
- Port: 25
- No TLS
- User / Pass: 

Secondary SMTP Server

- Host: smtp.gmail.com
- Port: 465
- TLS
- User / Pass: eventsen

Dial-Up / VPN Connection

- Dial: 
- Disconnect after

Limits

- Events per email: unlimited
Process Action
7.2.1.6 Remote Update Window
7.3 Event Log Reference

7.3.1 Security Events

7.3.1.1 Legacy Operating Systems

7.3.1.1.1 Windows NT Security Events

*Windows NT security event descriptions* from the security event log. These events will appear with the *security* event source.

- **Event ID:** 512
  - **Type:** Success Audit
  - **Description:** Windows NT is starting up.

- **Event ID:** 513
  - **Type:** Success Audit
  - **Description:** Windows NT is shutting down. All logon sessions will be terminated by this shutdown.

- **Event ID:** 514
  - **Type:** Success Audit
  - **Description:** An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.
  - **Authentication Package Name:** %1

- **Event ID:** 515
  - **Type:** Success Audit
  - **Description:** A trusted logon process has registered with the Local Security Authority. This logon process will be trusted to submit logon requests.
  - **Logon Process Name:** %1

- **Event ID:** 516
  - **Type:** Success Audit
  - **Description:** Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
  - **Number of audit messages discarded:** %1

- **Event ID:** 517
  - **Type:** Success Audit
  - **Description:** The audit log was cleared
  - **Primary User Name:** %1
  - **Primary Domain:** %2
  - **Primary Logon ID:** %3
  - **Client User Name:** %4
  - **Client Domain:** %5
  - **Client Logon ID:** %6

- **Event ID:** 518
  - **Type:** Success Audit
  - **Description:** A notification package has been loaded by the Security Account Manager. This package will be notified of any account or password changes.
  - **Notification Package Name:** %1

- **Event ID:** 528
  - **Type:** Success Audit
Description: Successful Logon:
User Name: %1          Domain: %2
Logon ID: %3           Logon Type: %4
Logon Process: %5      Authentication Package: %6
Workstation Name: %7

Event ID: 529
Type: Failure Audit
Description: Logon Failure:
Reason: Unknown user name or bad password
User Name: %1          Domain: %2
Logon Type: %3         Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 530
Type: Failure Audit
Description: Logon Failure:
Reason: Account logon time restriction violation
User Name: %1          Domain: %2
Logon Type: %3         Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 531
Type: Failure Audit
Description: Logon Failure:
Reason: Account currently disabled
User Name: %1          Domain: %2
Logon Type: %3         Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 532
Type: Failure Audit
Description: Logon Failure:
Reason: The specified user account has expired
User Name: %1          Domain: %2
Logon Type: %3         Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 533
Type: Failure Audit
Description: Logon Failure:
Reason: User not allowed to logon at this computer
User Name: %1          Domain: %2
Logon Type: %3         Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 534
Type: Failure Audit
Description: Logon Failure:
Reason: The user has not been granted the requested logon
type at this machine
User Name: %1          Domain: %2
Logon Type: %3         Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 535
Type: Failure Audit
Description: Logon Failure:
Reason: The specified account's password has expired
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 536
Type: Failure Audit

Description: Logon Failure:
Reason: The NetLogon component is not active
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 537
Type: Failure Audit

Description: Logon Failure:
Reason: An unexpected error occurred during logon
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 538
Type: Success Audit

Description: User Logoff:
User Name: %1              Domain: %2
Logon ID: %3              Logon Type: %4

Event ID: 539
Type: Failure Audit

Description: Logon Failure:
Reason: Account locked out
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 560
Type: Success Audit

Description: Object Open:
Object Server: %1          Object Type: %2
Object Name: %3            New Handle ID: %4
Operation ID: {%5,%6}
Process ID: %7             Primary User Name: %8
Primary Domain: %9         Primary Logon ID: %10
Client User Name: %11      Client Domain: %12
Client Logon ID: %13       Accesses %14
Privileges %15

Event ID: 561
Type: Success Audit

Description: Handle Allocated:
Handle ID: %1              Operation ID: {%2,%3}
Process ID: %4

Event ID: 562
Type: Success Audit
Description: Handle Closed:
Object Server: %1          Handle ID: %2
Process ID: %3

Event ID: 563
Type: Success Audit
Description: Object Open for Delete:
Object Server: %1          Object Type: %2
Object Name: %3            New Handle ID: %4
Operation ID: (%5,%6)
Process ID: %7             Primary User Name: %8
Primary Domain: %9         Primary Logon ID: %10
Client User Name: %11      Client Domain: %12
Client Logon ID: %13       Accesses %14
Privileges %15

Event ID: 564
Type: Success Audit
Description: Object Deleted:
Object Server: %1          Handle ID: %2
Process ID: %3

Event ID: 576
Type: Success Audit
Description: Special privileges assigned to new logon:
User Name: %1             Domain: %2
Logon ID: %3              Assigned: %4

Event ID: 577
Type: Success Audit
Description: Privileged Service Called:
Server: %1              Service: %2
Primary User Name: %3      Primary Domain: %4
Primary Logon ID: %5       Client User Name: %6
Client Domain: %7          Client Logon ID: %8
Privileges: %9

Event ID: 578
Type: Failure Audit
Description: Privileged object operation:
Object Server: %1          Object Handle: %2
Process ID: %3             Primary User Name: %4
Primary Domain: %5         Primary Logon ID: %6
Client User Name: %7       Client Domain: %8
Client Logon ID: %9        Privileges: %10

Event ID: 592
Type: Success Audit
Description: A new process has been created:
New Process ID: %1         Image File Name: %2
Creator Process ID: %3     User Name: %4
Domain: %5                 Logon ID: %6

Event ID: 593
Type: Success Audit
Description: A process has exited:
Process ID: %1             User Name: %2
Domain: %3                 Logon ID: %4
Event ID: 594  
Type: Success Audit  
Description: A handle to an object has been duplicated:  
Source Handle ID: %1 Source Process ID: %2  
Target Handle ID: %3 Target Process ID: %4

Event ID: 595  
Type: Success Audit  
Description: Indirect access to an object has been obtained:  
Object Type: %1 Object Name: %2  
Process ID: %3 Primary User Name: %4  
Primary Domain: %5 Primary Logon ID: %6  
Client User Name: %7 Client Domain: %8  
Client Logon ID: %9 Accesses: %10

Event ID: 608  
Type: Success Audit  
Description: User Right Assigned:  
User Right: %1 Assigned To: %2  
Assigned By:  
User Name: %3 Domain: %4  
Logon ID: %5

Event ID: 609  
Type: Success Audit  
Description: User Right Removed:  
User Right: %1 Removed From: %2  
Removed By:  
User Name: %3 Domain: %4  
Logon ID: %5

Event ID: 610  
Type: Success Audit  
Description: New Trusted Domain:  
Domain Name: %1 Domain ID: %2  
Established By:  
User Name: %3 Domain: %4  
Logon ID: %5

Event ID: 611  
Type: Success Audit  
Description: Removing Trusted Domain:  
Domain Name: %1 Domain ID: %2  
Removed By:  
User Name: %3 Domain: %4  
Logon ID: %5

Event ID: 612  
Type: Success Audit  
Description: Audit Policy Change:  
New Policy:  
Success Failure  
%1 %2 System  
%3 %4 Logon/Logoff  
%5 %6 Object Access  
%7 %8 Privilege Use
%9  %10  Detailed Tracking  
%11  %12  Policy Change  
%13  %14  Account Management  

Changed By:  
User Name: %15  Domain Name: %16  
Logon ID: %17  

Event ID: 624  
Type: Success Audit  
Description: User Account Created:  
New Account Name: %1  New Domain: %2  
New Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  
Privileges %7  

Event ID: 625  
Type: Success Audit  
Description: User Account Type Change:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  New Type: %4  
Caller User Name: %5  Caller Domain: %6  
Caller Logon ID: %7  

Event ID: 626  
Type: Success Audit  
Description: User Account Enabled:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  

Event ID: 627  
Type: Success Audit  
Description: Change Password Attempt:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  
Privileges: %7  

Event ID: 628  
Type: Success Audit  
Description: User Account password set:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  

Event ID: 629  
Type: Success Audit  
Description: User Account Disabled:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  

Event ID: 630  
Type: Success Audit  
Description: User Account Deleted:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4
Event ID: 631
Type: Success Audit
Description: Global Group Created:
New Account Name: %1
New Account ID: %3
Caller Domain: %5
Privileges: %7

Event ID: 632
Type: Success Audit
Description: Global Group Member Added:
Member: %1
Target Domain: %3
Target Account Name: %2
Caller User Name: %5
Caller Domain: %6
Caller Logon ID: %7
Privileges: %8

Event ID: 633
Type: Success Audit
Description: Global Group Member Removed:
Member: %1
Target Domain: %3
Target Account Name: %2
Caller User Name: %5
Caller Domain: %6
Caller Logon ID: %7
Privileges: %8

Event ID: 634
Type: Success Audit
Description: Global Group Deleted:
Target Account Name: %1
Target Domain: %3
Caller User Name: %5
Caller Domain: %6
Privileges: %7

Event ID: 635
Type: Success Audit
Description: Local Group Created:
New Account Name: %1
New Account ID: %3
Caller Domain: %5
Privileges: %7

Event ID: 636
Type: Success Audit
Description: Local Group Member Added:
Member: %1
Target Domain: %3
Target Account Name: %2
Caller User Name: %5
Caller Domain: %6
Caller Logon ID: %7
Privileges: %8

Event ID: 637
Type: Success Audit
Description: Local Group Member Removed:
Member: %1
Target Domain: %3
Target Account Name: %2
Caller User Name: %5
Caller Domain: %6
Caller Logon ID: %7  Privileges: %8

Event ID: 638  
Type: Success Audit  
Description: Local Group Deleted:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  
Privileges: %7

Event ID: 639  
Type: Success Audit  
Description: Local Group Changed:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  
Privileges: %7

Event ID: 640  
Type: Success Audit  
Description: General Account Database Change:  
Type of change: %1  Object Type: %2  
Object Name: %3  Object ID: %4  
Caller User Name: %5  Caller Domain: %6  
Caller Logon ID: %7

Event ID: 641  
Type: Success Audit  
Description: Global Group Changed:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  
Privileges: %7

Event ID: 642  
Type: Success Audit  
Description: User Account Changed:  
Target Account Name: %1  Target Domain: %2  
Target Account ID: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6  
Privileges: %7

Event ID: 643  
Type: Success Audit  
Description: Domain Policy Changed:  
Domain: %1  Domain ID: %2  
Caller User Name: %3  Caller Domain: %4  
Caller Logon ID: %5  Privileges: %6

Event ID: 644  
Type: Success Audit  
Description: User Account Locked Out  
Target Account Name: %1  Target Account ID: %2  
Caller Machine Name: %3  Caller User Name: %4  
Caller Domain: %5  Caller Logon ID: %6
7.3.1.1.2 Windows 2000 Security Events

**Windows 2000 security event descriptions** from the security event log. These events will appear with the **security** event source. Most of the event descriptions listed here also apply to Windows XP and Windows Server 2003.

- **Event ID: 512 (0x0200)**
  Type: Success Audit
  Description: Windows NT is starting up.

- **Event ID: 513 (0x0201)**
  Type: Success Audit
  Description: Windows NT is shutting down.
  All logon sessions will be terminated by this shutdown.

- **Event ID: 514 (0x0202)**
  Type: Success Audit
  Description: An authentication package has been loaded by the Local Security Authority.
  This authentication package will be used to authenticate logon attempts.
  Authentication Package Name: %1

- **Event ID: 515 (0x0203)**
  Type: Success Audit
  Description: A trusted logon process has registered with the Local Security Authority.
  This logon process will be trusted to submit logon requests.
  Logon Process Name: %1

- **Event ID: 516 (0x0204)**
  Type: Success Audit
  Description: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
  Number of audit messages discarded: %1

- **Event ID: 517 (0x0205)**
  Type: Success Audit
  Description: The audit log was cleared
  Primary User Name: %1     Primary Domain: %2
  Primary Logon ID: %3     Client User Name: %4
  Client Domain: %5     Client Logon ID: %6

- **Event ID: 518 (0x0206)**
  Type: Success Audit
  Description: An notification package has been loaded by the Security Account Manager.
  This package will be notified of any account or password changes.
  Notification Package Name: %1

- **Event ID: 528 (0x0210)**
  Type: Success Audit
  Description: Successful Logon:
  User Name: %1     Domain: %2
  Logon ID: %3     Logon Type: %4
  Logon Process: %5     Authentication Package: %6
  Workstation Name: %7

- **Event ID: 529 (0x0211)**
  Type: Failure Audit
Description: Logon Failure
Reason: Unknown user name or bad password
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 530 (0x0212)
Type: Failure Audit
Description: Logon Failure
Reason: Account logon time restriction violation
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 531 (0x0213)
Type: Failure Audit
Description: Logon Failure
Reason: Account currently disabled
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 532 (0x0214)
Type: Failure Audit
Description: Logon Failure
Reason: The specified user account has expired
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 533 (0x0215)
Type: Failure Audit
Description: Logon Failure
Reason: User not allowed to logon at this computer
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 534 (0x0216)
Type: Failure Audit
Description: Logon Failure
Reason: The user has not been granted the requested logon type at this machine
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 535 (0x0217)
Type: Failure Audit
Description: Logon Failure
Reason: The specified account's password has expired
User Name: %1              Domain: %2
Logon Type: %3             Logon Process: %4
Authentication Package: %5 Workstation Name: %6

Event ID: 536 (0x0218)
Type: Failure Audit
Description: Logon Failure
Reason: The NetLogon component is not active
User Name: %1  Domain: %2
Logon Type: %3  Logon Process: %4
Authentication Package: %5  Workstation Name: %6

Event ID: 537 (0x0219)
Type: Failure Audit
Description: Logon Failure
Reason: An unexpected error occurred during logon
User Name: %1  Domain: %2
Logon Type: %3  Logon Process: %4
Authentication Package: %5  Workstation Name: %6

Event ID: 538 (0x021A)
Type: Success Audit
Description: User Logoff
User Name: %1  Domain: %2
Logon ID: %3  Logon Type: %4.

Event ID: 539 (0x021B)
Type: Failure Audit
Description: Logon Failure
Reason: Account locked out
User Name: %1  Domain: %2
Logon Type: %3  Logon Process: %4
Authentication Package: %5  Workstation Name: %6

Event ID: 540 (0x021C)
Type: Success Audit
Description: Successful Network Logon
User Name: %1  Domain: %2
Logon ID: %3  Logon Type: %4
Logon Process: %5  Authentication Package: %6
Workstation Name: %7

Event ID: 541 (0x021D)
Type: Success Audit
Description: IKE security association established.
Mode: %1  Peer Identity: %2
Filter: %3  Parameters: %4

Event ID: 542 (0x021E)
Type: Success Audit
Description: IKE security association ended.
Mode: Data Protection (Quick mode)
Filter: %1  Inbound SPI: %2
Outbound SPI: %3

Event ID: 543 (0x021F)
Type: Success Audit
Description: IKE security association ended.
Mode: Key Exchange (Main mode)
Filter: %1

Event ID: 544 (0x0220)
Type: Failure Audit
Description: IKE security association establishment failed because peer could not authenticate. The certificate trust could not be established.

Peer Identity: %1          Filter: %2

Event ID: 545 (0x0221)
Type: Failure Audit
Description: IKE peer authentication failed.

Peer Identity: %1          Filter: %2

Event ID: 546 (0x0222)
Type: Failure Audit
Description: IKE security association establishment failed because peer sent invalid proposal.

Mode: %1                   Filter: %2
Attribute: %3              Expected value: %4
Received value: %5

Event ID: 547 (0x0223)
Type: Failure Audit
Description: IKE security association negotiation failed.

Mode: %1                   Filter: %2
Failure Point: %3          Failure Reason: %4

Event ID: 560 (0x0230)
Type: Success Audit
Description: Object Open

Object Server: %1          Object Type: %2
Object Name: %3            New Handle ID: %4
Operation ID:{%5,%6}       Process ID: %7
Primary User Name: %8      Primary Domain: %9
Primary Logon ID: %10      Client User Name: %11
Client Domain: %12         Client Logon ID: %13
Accesses %14               Privileges %15

Event ID: 561 (0x0231)
Type: Success Audit
Description: Handle Allocated

Handle ID: %1              Operation ID:{%2,%3}
Process ID: %4

Event ID: 562 (0x0232)
Type: Success Audit
Description: Handle Closed

Object Server: %1          Handle ID: %2
Process ID: %3

Event ID: 563 (0x0233)
Type: Success Audit
Description: Object Open for Delete

Object Server: %1          Object Type: %2
Object Name: %3            New Handle ID: %4
Operation ID:{%5,%6}       Process ID: %7
Primary User Name: %8      Primary Domain: %9
Primary Logon ID: %10      Client User Name: %11
Client Domain: %12         Client Logon ID: %13
Accesses %14               Privileges %15
Event ID: 564 (0x0234)  
Type: Success Audit  
Description: Object Deleted  
Object Server: %1 Handle ID: %2 
Process ID: %3

Event ID: 565 (0x0235)  
Type: Success Audit  
Description: Object Open  
Object Server: %1 Object Type: %2 
Object Name: %3 New Handle ID: %4 
Operation ID:{%5,%6} Process ID: %7 
Primary User Name: %8 Primary Domain: %9 
Primary Logon ID: %10 Client User Name: %11 
Client Domain: %12 Client Logon ID: %13 
Accesses %14 Privileges %15 
Properties:%16%17%18%19%20%21%22%23%24%25

Event ID: 566 (0x0236)  
Type: Success Audit  
Description: Object Operation  
Operation Type %1 Object Type: %2 
Object Name: %3 Handle ID: %4 
Operation ID:{%5,%6} Primary User Name: %7 
Primary Domain: %8 Primary Logon ID: %9 
Client User Name: %10 Client Domain: %11 
Client Logon ID: %12 Requested Accesses %13

Event ID: 576 (0x0240)  
Type: Success Audit  
Description: Special privileges assigned to new logon:  
User Name: %1 Domain: %2 
Logon ID: %3 Assigned: %4

Event ID: 577 (0x0241)  
Type: Success Audit  
Description: Privileged Service Called  
Server: %1 Service: %2 
Primary User Name: %3 Primary Domain: %4 
Primary Logon ID: %5 Client User Name: %6 
Client Domain: %7 Client Logon ID: %8 
Privileges: %9

Event ID: 578 (0x0242)  
Type: Success Audit  
Description: Privileged object operation  
Object Server: %1 Object Handle: %2 
Process ID: %3 Primary User Name: %4 
Primary Domain: %5 Primary Logon ID: %6 
Client User Name: %7 Client Domain: %8 
Client Logon ID: %9 Privileges: %10

Event ID: 592 (0x0250)  
Type: Success Audit  
Description: A new process has been created  
New Process ID: %1 Image File Name: %2 
Creator Process ID: %3 User Name: %4
Event ID: 593 (0x0251)
Type: Success Audit
Description: A process has exited
Process ID: %1 User Name: %2
Domain: %3 Logon ID: %4

Event ID: 594 (0x0252)
Type: Success Audit
Description: A handle to an object has been duplicated
Source Handle ID: %1 Source Process ID: %2
Target Handle ID: %3 Target Process ID: %4

Event ID: 595 (0x0253)
Type: Success Audit
Description: Indirect access to an object has been obtained
Object Type: %1 Object Name: %2
Process ID: %3 Primary User Name: %4
Primary Domain: %5 Primary Logon ID: %6
Client User Name: %7 Client Domain: %8
Client Logon ID: %9 Accesses: %10

Event ID: 608 (0x0260)
Type: Success Audit
Description: User Right Assigned
User Right: %1 Assigned To: %2
Assigned By User Name: %3 Domain: %4
Logon ID: %5

Event ID: 609 (0x0261)
Type: Success Audit
Description: User Right Removed
User Right: %1 Removed From: %2
Removed By User Name: %3 Domain: %4
Logon ID: %5

Event ID: 610 (0x0262)
Type: Success Audit
Description: New Trusted Domain
Domain Name: %1 Domain ID: %2
Established By:
User Name: %3 Domain: %4
Logon ID: %5

Event ID: 611 (0x0263)
Type: Success Audit
Description: Removing Trusted Domain
Domain Name: %1 Domain ID: %2
Removed By User Name: %3 Domain: %4
Logon ID: %5

Event ID: 612 (0x0264)
Type: Success Audit
Description: Audit Policy Change
New Policy:
Success Failure
%1 %2 System
%3 %4 Logon/Logoff
%5 %6 Object Access
%7 %8 Privilege Use
%9 %10 Detailed Tracking
%11 %12 Policy Change
%13 %14 Account Management

Changed By:
User Name: %15 Domain Name: %16
Logon ID: %17

Event ID: 613 (0x0265)
Type: Success Audit
Description: IPSec policy agent started
Ipsec Policy Agent: %1 Policy Source: %2
Event Data: %3

Event ID: 614 (0x0266)
Type: Success Audit
Description: IPSec policy agent disabled
Ipsec Policy Agent: %1 Event Data: %2

Event ID: 615 (0x0267)
Type: Success Audit
Description: IPSEC PolicyAgent Service: %1
Event Data: %1

Event ID: 616 (0x0268)
Type: Failure Audit
Description: IPSec policy agent encountered a potentially serious failure.
Event Data: %1

Event ID: 617 (0x0269)
Type: Success Audit
Description: Kerberos Policy Changed
Changed By: User Name: %1 Domain Name: %2
Logon ID: %3
Changes made: %4

'-' means no changes, otherwise each change is shown as:
Parameter Name: (new value) (old value)

Event ID: 618 (0x026a)
Type: Success Audit
Description: Encrypted Data Recovery Policy Changed
Changed By: User Name: %1 Domain Name: %2
Logon ID: %3
Changes made: %4

'-' means no changes, otherwise each change is shown as:
Parameter Name: new value (old value)

Event ID: 619 (0x026b)
Type: Success Audit
Description: Quality of Service Policy Changed
Changed By: User Name: %1 Domain Name: %2
Logon ID: %3
Changes made: %4

'-' means no changes, otherwise each change is shown as:
Parameter Name: new value (old value)

Event ID: 620 (0x026C)
Description: Trusted Domain Information Modified:
Domain Name: %1            Domain ID: %2
Modified By: User Name: %3              Domain: %4
Logon ID: %5

Event ID: 624 (0x0270)
Type: Success Audit
Description: User Account Created
New Account Name: %1       New Domain: %2
New Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges %7

Event ID: 625 (0x0271)
Description: User Account Type Change
Type: Success Audit
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
New Type: %4               Caller User Name: %5
Caller Domain: %6          Caller Logon ID: %7

Event ID: 626 (0x0272)
Description: User Account Enabled
Type: Success Audit
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6

Note: Windows 2000 does not log event ID 626 explicitly.
Results are logged as a part of event ID 642 in the description of the message.

Event ID: 627 (0x0273)
Type: Success Audit
Description: Change Password Attempt
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 628 (0x0274)
Type: Success Audit
Description: User Account password set
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6

Event ID: 630 (0x0276)
Type: Success Audit
Description: User Account Deleted:
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 631 (0x0277)
Type: Success Audit
Description: Security Enabled Global Group Created
New Account Name: %1       New Domain: %2
New Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 632 (0x0278)
Type: Success Audit
Description: Security Enabled Global Group Member Added
Member Name: %1            Member ID: %2
Target Account Name: %3    Target Domain: %4
Target Account ID: %5
Caller User Name: %6       Caller Domain: %7
Caller Logon ID: %8        Privileges: %9

Event ID: 633 (0x0279)
Type: Success Audit
Description: Security Enabled Global Group Member Removed
Member Name: %1            Member ID: %2
Target Account Name: %3    Target Domain: %4
Target Account ID: %5
Caller User Name: %6       Caller Domain: %7
Caller Logon ID: %8        Privileges: %9

Event ID: 634 (0x027A)
Type: Success Audit
Description: Security Enabled Global Group Deleted
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 635 (0x027B)
Type: Success Audit
Description: Security Enabled Local Group Created
New Account Name: %1       New Domain: %2
New Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 636 (0x027C)
Type: Success Audit
Description: Security Enabled Local Group Member Added
Member Name: %1            Member ID: %2
Target Account Name: %3    Target Domain: %4
Target Account ID: %5
Caller User Name: %6       Caller Domain: %7
Caller Logon ID: %8        Privileges: %9
Event ID: 637 (0x027D)
Type: Success Audit
Description: Security Enabled Local Group Member Removed
Member Name: %1 Member ID: %2
Target Account Name: %3 Target Domain: %4
Target Account ID: %5
Caller User Name: %6 Caller Domain: %7
Caller Logon ID: %8 Privileges: %9

Event ID: 638 (0x027E)
Type: Success Audit
Description: Security Enabled Local Group Deleted
Target Account Name: %1 Target Domain: %2
Target Account ID: %3
Caller User Name: %4 Caller Domain: %5
Caller Logon ID: %6 Privileges: %7

Event ID: 639 (0x027F)
Type: Success Audit
Description: Security Enabled Local Group Changed
Target Account Name: %1 Target Domain: %2
Target Account ID: %3
Caller User Name: %4 Caller Domain: %5
Caller Logon ID: %6 Privileges: %7

Event ID: 640 (0x0280)
Type: Success Audit
Description: General Account Database Change
Type of change: %1 Object Type: %2
Object Name: %3 Object ID: %4
Caller User Name: %5 Caller Domain: %6
Caller Logon ID: %7

Event ID: 641 (0x0281)
Type: Success Audit
Description: Security Enabled Global Group Changed
Target Account Name: %1 Target Domain: %2
Target Account ID: %3
Caller User Name: %4 Caller Domain: %5
Caller Logon ID: %6 Privileges: %7

Event ID: 642 (0x0282)
Type: Success Audit
Description: User Account Changed
Target Account Name: %1 Target Domain: %2
Target Account ID: %3
Caller User Name: %4 Caller Domain: %5
Caller Logon ID: %6 Privileges: %7

Event ID: 643 (0x0283)
Type: Success Audit
Description: Domain Policy Changed: %1 modified
Domain: %2 Domain ID: %3
Caller User Name: %4 Caller Domain: %5
Caller Logon ID: %6 Privileges: %7

Event ID: 644 (0x0284)
Type: Success Audit
Description: User Account Locked Out
Target Account Name: %1    Target Account ID: %3
Caller Machine Name: %2
Caller User Name: %4    Caller Domain: %5
Caller Logon ID: %6

Event ID: 645 (0x0285)

Type: Success Audit
Description: Computer Account Created
New Account Name: %1    New Domain: %2
New Account ID: %3
Caller User Name: %4    Caller Domain: %5
Caller Logon ID: %6
Privileges %7

Event ID: 646 (0x0286)

Type: Success Audit
Description: Computer Account Changed
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %5    Caller Domain: %6
Caller Logon ID: %7
Privileges: %8

Event ID: 647 (0x0287)

Type: Success Audit
Description: Computer Account Deleted
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4    Caller Domain: %5
Caller Logon ID: %6
Privileges: %7

Event ID: 648 (0x0288)

Type: Success Audit
Description: Security Disabled Local Group Created
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4    Caller Domain: %5
Caller Logon ID: %6
Privileges: %7

Event ID: 649 (0x0289)

Type: Success Audit
Description: Security Disabled Local Group Changed
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4    Caller Domain: %5
Caller Logon ID: %6
Privileges: %7

Event ID: 650 (0x028A)

Type: Success Audit
Description: Security Disabled Local Group Member Added
Member Name: %1    Member ID: %2
Target Account Name: %3    Target Domain: %4
Target Account ID: %5
Caller User Name: %6    Caller Domain: %7
Caller Logon ID: %8
Privileges: %9

Event ID: 651 (0x028B)
Type: Success Audit
Description: Security Disabled Local Group Member Removed
Member Name: %1               Member ID: %2
Target Account Name: %3       Target Domain: %4
Target Account ID: %5
Caller User Name: %6          Caller Domain: %7
Caller Logon ID: %8           Privileges: %9

Event ID: 652 (0x028C)
Type: Success Audit
Description: Security Disabled Local Group Deleted
Target Account Name: %1       Target Domain: %2
Target Account ID: %3
Caller User Name: %4          Caller Domain: %5
Caller Logon ID: %6           Privileges: %7

Event ID: 653 (0x028D)
Type: Success Audit
Description: Security Disabled Global Group Created
New Account Name: %1          New Domain: %2
New Account ID: %3
Caller User Name: %4          Caller Domain: %5
Caller Logon ID: %6           Privileges: %7

Event ID: 654 (0x028E)
Type: Success Audit
Description: Security Disabled Global Group Changed
Target Account Name: %1       Target Domain: %2
Target Account ID: %3
Caller User Name: %4          Caller Domain: %5
Caller Logon ID: %6           Privileges: %7

Event ID: 655 (0x028F)
Type: Success Audit
Description: Security Disabled Global Group Member Added
Member Name: %1               Member ID: %2
Target Account Name: %3       Target Domain: %4
Target Account ID: %5
Caller User Name: %6          Caller Domain: %7
Caller Logon ID: %8           Privileges: %9

Event ID: 656 (0x0290)
Type: Success Audit
Description: Security Disabled Global Group Member Removed
Member Name: %1               Member ID: %2
Target Account Name: %3       Target Domain: %4
Target Account ID: %5
Caller User Name: %6          Caller Domain: %7
Caller Logon ID: %8           Privileges: %9

Event ID: 657 (0x0291)
Type: Success Audit
Description: Security Disabled Global Group Deleted
Target Account Name: %1       Target Domain: %2
Target Account ID: %3
Caller User Name: %4          Caller Domain: %5
Caller Logon ID: %6           Privileges: %7
Event ID: 658 (0x0292)
Type: Success Audit
Description: Security Enabled Universal Group Created
New Account Name: %1       New Domain: %2
New Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 659 (0x0293)
Type: Success Audit
Description: Security Enabled Universal Group Changed
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 660 (0x0294)
Type: Success Audit
Description: Security Enabled Universal Group Member Added
Member Name: %1            Member ID: %2
Target Account Name: %3    Target Domain: %4
Target Account ID: %5
Caller User Name: %6       Caller Domain: %7
Caller Logon ID: %8        Privileges: %9

Event ID: 661 (0x0295)
Type: Success Audit
Description: Security Enabled Universal Group Member Removed
Member Name: %1            Member ID: %2
Target Account Name: %3    Target Domain: %4
Target Account ID: %5
Caller User Name: %6       Caller Domain: %7
Caller Logon ID: %8        Privileges: %9

Event ID: 662 (0x0296)
Type: Success Audit
Description: Security Enabled Universal Group Deleted
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 663 (0x0297)
Type: Success Audit
Description: Security Disabled Universal Group Created
New Account Name: %1       New Domain: %2
New Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6        Privileges: %7

Event ID: 664 (0x0298)
Type: Success Audit
Description: Security Disabled Universal Group Changed
Target Account Name: %1    Target Domain: %2
Target Account ID: %3
Caller User Name: %4       Caller Domain: %5
Caller Logon ID: %6  Privileges: %7

Event ID: 665 (0x0299)
Type: Success Audit
Description: Security Disabled Universal Group Member Added
Member Name: %1  Member ID: %2
Target Account Name: %3  Target Domain: %4
Target Account ID: %5
Caller User Name: %6  Caller Domain: %7
Caller Logon ID: %8  Privileges: %9

Event ID: 666 (0x029A)
Type: Success Audit
Description: Security Disabled Universal Group Member Removed
Member Name: %1  Member ID: %2
Target Account Name: %3  Target Domain: %4
Target Account ID: %5
Caller User Name: %6  Caller Domain: %7
Caller Logon ID: %8  Privileges: %9

Event ID: 667 (0x029B)
Type: Success Audit
Description: Security Disabled Universal Group Deleted
Target Account Name: %1  Target Domain: %2
Target Account ID: %3
Caller User Name: %4  Caller Domain: %5
Caller Logon ID: %6  Privileges: %7

Event ID: 668 (0x029C)
Type: Success Audit
Description: Group Type Changed
Target Account Name: %1  Target Domain: %2
Target Account ID: %3
Caller User Name: %5  Caller Domain: %6
Caller Logon ID: %7  Privileges: %8

Event ID: 669 (0x029D)
Type: Success Audit
Description: Add SID History
Source Account Name: %1  Source Account ID: %2
Target Account Name: %3  Target Domain: %4
Target Account ID: %5
Caller User Name: %6  Caller Domain: %7
Caller Logon ID: %8  Privileges: %9

Event ID: 670 (0x029E)
Type: Success Audit
Description: Add SID History
Source Account Name: %1  Target Account Name: %2
Target Domain: %3  Target Account ID: %4
Caller User Name: %5  Caller Domain: %6
Caller Logon ID: %7  Privileges: %8

Event ID: 672 (0x02a0)
Type: Success Audit
Description: Authentication Ticket Granted
User Name: %1  Supplied Realm Name: %2
Event ID: 673 (0x02a1)
Type: Success Audit
Description: Service Ticket Granted
User Name: %1              User Domain: %2
Service Name: %3           Service ID: %4
Ticket Options: %5         Ticket Encryption Type: %6
Client Address: %7

Event ID: 674 (0x02a2)
Type: Success Audit
Description: Ticket Granted Renewed
User Name: %1              User Domain: %2
Service Name: %3           Service ID: %4
Ticket Options: %5         Ticket Encryption Type: %6
Client Address: %7

Event ID: 675 (0x02a3)
Type: Failure Audit
Description: Pre-authentication failed
User Name: %1              User ID: %2
Service Name: %3           Pre-Authentication Type: %4
Failure Code: %5           Client Address: %6

Event ID: 676 (0x02a4)
Type: Failure Audit
Description: Authentication Ticket Request Failed
User Name: %1              Supplied Realm Name: %2
Service Name: %3           Ticket Options: %4
Failure Code: %5           Client Address: %6

Event ID: 677 (0x02a5)
Type: Failure Audit
Description: Service Ticket Request Failed:
User Name: %1              Supplied Realm Name: %2
Service Name: %3           Ticket Options: %4
Failure Code: %5           Client Address: %6

Event ID: 678 (0x02a6)
Type: Success Audit
Description: Account Mapped for Logon by: %1
Client Name: %2            Mapped Name: %3

Event ID: 679 (0x02a7)
Type: Failure Audit
Description: The name: %2 could not be mapped for logon by: %1

Event ID: 680 (0x02a8)
Type: Success Audit
Description: Account Used for Logon by: %1
Account Name: %2           Workstation: %3
Event ID: 681 (0x02a9)
Type: Failure Audit
Description: The logon to account: %2 by: %1 from workstation: %3 failed. The error code was: %4

Event ID: 682 (0x02aa)
Type: Success Audit
Description: Session reconnected to winstation:
  User Name: %1    Domain: %2
  Logon ID: %3    Session Name: %4
  Client Name: %5    Client Address: %6

Event ID: 683 (0x02ab)
Type: Success Audit
Description: Session disconnected from winstation:
  User Name: %1    Domain: %2
  Logon ID: %3    Session Name: %4
  Client Name: %5    Client Address: %6
7.3.1.2 Windows 2003 Security Events

**Account Logon Events**

Event ID: 672
Description: An authentication service (AS) ticket was successfully issued and validated.

Event ID: 673
A ticket granting service (TGS) ticket was granted. A TGS is a ticket issued by the Kerberos version 5 ticket-granting service TGS that allows a user to authenticate to a specific service in the domain.

Event ID: 674
A security principal renewed an AS ticket or TGS ticket.

Event ID: 675
Pre-authentication failed. This event is generated on a Key Distribution Center (KDC) when a user types in an incorrect password.

Event ID: 676
Authentication ticket request failed. This event is not generated in Windows XP Professional or in members of the Windows Server family.

Event ID: 677
A TGS ticket was not granted. This event is not generated in Windows XP Professional or in the members of the Windows Server family.

Event ID: 678
An account was successfully mapped to a domain account.

Event ID: 681
Logon failure. A domain account logon was attempted. This event is not generated in Windows XP Professional or in members of the Windows Server family.

Event ID: 682
A user has reconnected to a disconnected terminal server session.

Event ID: 683
A user disconnected a terminal server session without logging off.

**Account Management Events**

Event ID: 624
A user account was created.

Event ID: 627
A user password was changed.

Event ID: 628
A user password was set.

Event ID: 630
A user account was deleted.

Event ID: 631
A global group was created.
Event ID: 632
A member was added to a global group.

Event ID: 633
A member was removed from a global group.

Event ID: 634
A global group was deleted.

Event ID: 635
A new local group was created.

Event ID: 636
A member was added to a local group.

Event ID: 637
A member was removed from a local group.

Event ID: 638
A local group was deleted.

Event ID: 639
A local group account was changed.

Event ID: 641
A global group account was changed.

Event ID: 642
A user account was changed.

Event ID: 643
A domain policy was modified.

Event ID: 644
A user account was automatically locked.

Event ID: 645
A computer account was created.

Event ID: 646
A computer account was changed.

Event ID: 647
A computer account was deleted.

Event ID: 648
A local security group with security disabled was created.

Note: SECURITY_DISABLED in the formal name means that this group cannot be used to grant permissions in access checks.

Event ID: 649
A local security group with security disabled was changed.

Event ID: 650
A member was added to a security-disabled local security group.
Event ID: 651
A member was removed from a security-disabled local security group.

Event ID: 652
A security-disabled local group was deleted.

Event ID: 653
A security-disabled global group was created.

Event ID: 654
A security-disabled global group was changed.

Event ID: 655
A member was added to a security-disabled global group.

Event ID: 656
A member was removed from a security-disabled global group.

Event ID: 657
A security-disabled global group was deleted.

Event ID: 658
A security-enabled universal group was created.

Event ID: 659
A security-enabled universal group was changed.

Event ID: 660
A member was added to a security-enabled universal group.

Event ID: 661
A member was removed from a security-enabled universal group.

Event ID: 662
A security-enabled universal group was deleted.

Event ID: 663
A security-disabled universal group was created.

Event ID: 664
A security-disabled universal group was changed.

Event ID: 665
A member was added to a security-disabled universal group.

Event ID: 666
A member was removed from a security-disabled universal group.

Event ID: 667
A security-disabled universal group was deleted.

Event ID: 668
A group type was changed.

Event ID: 684
The security descriptor of administrative group members was set.
Note: Every 60 minutes on a domain controller, a background thread searches all members of administrative groups (such as domain, enterprise, and schema administrators) and applies a fixed security descriptor on them. This event is logged.

Event ID: 685
Name of an account was changed.

Directory Service Access Events

Event ID: 566
A generic object operation took place.

Audit Logon Events

Event ID: 528
A user successfully logged on to a computer.

Event ID: 529
Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.

Event ID: 530
Logon failure. A logon attempt was made outside the allowed time.

Event ID: 531
Logon failure. A logon attempt was made using a disabled account.

Event ID: 532
Logon failure. A logon attempt was made using an expired account.

Event ID: 533
Logon failure. A logon attempt was made by a user who is not allowed to log on at the specified computer.

Event ID: 534
Logon failure. The user attempted to log on with a password type that is not allowed.

Event ID: 535
Logon failure. The password for the specified account has expired.

Event ID: 536
Logon failure. The Net Logon service is not active.

Event ID: 537
Logon failure. The logon attempt failed for other reasons.

Note: In some cases, the reason for the logon failure may not be known.

Event ID: 538
The logoff process was completed for a user.

Event ID: 539
Logon failure. The account was locked out at the time the logon attempt was made.

Event ID: 540
A user successfully logged on to a network.
Event ID: 541
Main mode Internet Key Exchange (IKE) authentication was completed between the local computer and the listed peer identity (establishing a security association), or quick mode has established a data channel.

Event ID: 542
A data channel was terminated.

Event ID: 543
Main mode was terminated.

*Note: This might occur as a result of the time limit on the security association expiring (the default is eight hours), policy changes, or peer termination.*

Event ID: 544
Main mode authentication failed because the peer did not provide a valid certificate or the signature was not validated.

Event ID: 545
Main mode authentication failed because of a Kerberos failure or a password that is not valid.

Event ID: 546
IKE security association establishment failed because the peer sent a proposal that is not valid. A packet was received that contained data that is not valid.

Event ID: 547
A failure occurred during an IKE handshake.

Event ID: 548
Logon failure. The security identifier (SID) from a trusted domain does not match the account domain SID of the client.

Event ID: 549
Logon failure. All SIDs corresponding to untrusted namespaces were filtered out during an authentication across forests.

Event ID: 550
Notification message that could indicate a possible denial-of-service (DoS) attack.

Event ID: 551
A user initiated the logoff process.

Event ID: 552
A user successfully logged on to a computer using explicit credentials while already logged on as a different user.

Event ID: 682
A user has reconnected to a disconnected terminal server session.

Event ID: 683
A user disconnected a terminal server session without logging off.

*Note: This event is generated when a user is connected to a terminal server session over the network. It appears on the terminal server.*

**Object Access Events**

Event ID: 560
Access was granted to an already existing object.

Event ID: 562
A handle to an object was closed.

Event ID: 563
An attempt was made to open an object with the intent to delete it.

*Note: This is used by file systems when the FILE_DELETE_ON_CLOSE flag is specified in Createfile().*

Event ID: 564
A protected object was deleted.

Event ID: 565
Access was granted to an already existing object type.

Event ID: 567
A permission associated with a handle was used.

*Note: A handle is created with certain granted permissions (Read, Write, and so on). When the handle is used, up to one audit is generated for each of the permissions that were used.*

Event ID: 568
An attempt was made to create a hard link to a file that is being audited.

Event ID: 569
The resource manager in Authorization Manager attempted to create a client context.

Event ID: 570
A client attempted to access an object.

*Note: An event will be generated for every attempted operation on the object.*

Event ID: 571
The client context was deleted by the Authorization Manager application.

Event ID: 572
The Administrator Manager initialized the application.

Event ID: 772
The Certificate Manager denied a pending certificate request.

Event ID: 773
Certificate Services received a resubmitted certificate request.

Event ID: 774
Certificate Services revoked a certificate.

Event ID: 775
Certificate Services received a request to publish the certificate revocation list (CRL).

Event ID: 776
Certificate Services published the CRL.

Event ID: 777
A certificate request extension was made.
Event ID: 778
One or more certificate request attributes changed.

Event ID: 779
Certificate Services received a request to shut down.

Event ID: 780
Certificate Services backup started.

Event ID: 781
Certificate Services backup completed.

Event ID: 782
Certificate Services restore started.

Event ID: 783
Certificate Services restore completed.

Event ID: 784
Certificate Services started.

Event ID: 785
Certificate Services stopped.

Event ID: 786
The security permissions for Certificate Services changed.

Event ID: 787
Certificate Services retrieved an archived key.

Event ID: 788
Certificate Services imported a certificate into its database.

Event ID: 789
The audit filter for Certificate Services changed.

Event ID: 790
Certificate Services received a certificate request.

Event ID: 791
Certificate Services approved a certificate request and issued a certificate.

Event ID: 792
Certificate Services denied a certificate request.

Event ID: 793
Certificate Services set the status of a certificate request to pending.

Event ID: 794
The certificate manager settings for Certificate Services changed.

Event ID: 795
A configuration entry changed in Certificate Services.

Event ID: 796
A property of Certificate Services changed.
Event ID: 797
Certificate Services archived a key.

Event ID: 798
Certificate Services imported and archived a key.

Event ID: 799
Certificate Services published the certificate authority (CA) certificate to Microsoft Active Directory directory service.

Event ID: 800
One or more rows have been deleted from the certificate database.

Event ID: 801
Role separation enabled.

**Audit Policy Change Events**

Event ID: 608
A user right was assigned.

Event ID: 609
A user right was removed.

Event ID: 610
A trust relationship with another domain was created.

Event ID: 611
A trust relationship with another domain was removed.

Event ID: 612
An audit policy was changed.

Event ID: 613
An Internet Protocol security (IPSec) policy agent started.

Event ID: 614
An IPSec policy agent was disabled.

Event ID: 615
An IPSec policy agent changed.

Event ID: 616
An IPSec policy agent encountered a potentially serious failure.

Event ID: 617
A Kerberos version 5 policy changed.

Event ID: 618
Encrypted Data Recovery policy changed.

Event ID: 620
A trust relationship with another domain was modified.

Event ID: 621
System access was granted to an account.
Event ID: 622
System access was removed from an account.

Event ID: 623
Auditing policy was set on a per-user basis

Event ID: 625
Auditing policy was refreshed on a per-user basis.

Event ID: 768
A collision was detected between a namespace element in one forest and a namespace element in another forest.

Note: When a namespace element in one forest overlaps a namespace element in another forest, it can lead to ambiguity in resolving a name belonging to one of the namespace elements. This overlap is also called a collision. Not all parameters are valid for each entry type. For example, fields such as DNS name, NetBIOS name, and SID are not valid for an entry of type 'TopLevelName.'

Event ID: 769
Trusted forest information was added.

Note: This event message is generated when forest trust information is updated and one or more entries are added. One event message is generated for each added, deleted, or modified entry. If multiple entries are added, deleted, or modified in a single update of the forest trust information, all the generated event messages are assigned a single unique identifier called an operation ID. This allows you to determine that the multiple generated event messages are the result of a single operation. Not all parameters are valid for each entry type. For example, parameters such as DNS name, NetBIOS name and SID are not valid for an entry of type "TopLevelName."

Event ID: 770
Trusted forest information was deleted.

Note: See event description for event 769.

Event ID: 771
Trusted forest information was modified.

Note: See event description for event 769.

Event ID: 805
The event log service read the security log configuration for a session.

Privilege Use Events

Event ID: 576
Specified privileges were added to a user's access token.

Note: This event is generated when the user logs on.

Event ID: 577
A user attempted to perform a privileged system service operation.

Event ID: 578
Privileges were used on an already open handle to a protected object.

Detailed Tracking Events
Event ID: 592
A new process was created.

Event ID: 593
A process exited.

Event ID: 594
A handle to an object was duplicated.

Event ID: 595
Indirect access to an object was obtained.

Event ID: 596
A data protection master key was backed up.

Note: The master key is used by the CryptProtectData and CryptUnprotectData routines, and Encrypting File System (EFS). The master key is backed up each time a new one is created. (The default setting is 90 days.) The key is usually backed up by a domain controller.

Event ID: 597
A data protection master key was recovered from a recovery server.

Event ID: 598
Auditable data was protected.

Event ID: 599
Auditable data was unprotected.

Event ID: 600
A process was assigned a primary token.

Event ID: 601
A user attempted to install a service.

Event ID: 602
A scheduler job was created.

**Audit System Events**

Event ID: 512
Windows is starting up.

Event ID: 513
Windows is shutting down.

Event ID: 514
An authentication package was loaded by the Local Security Authority.

Event ID: 515
A trusted logon process has registered with the Local Security Authority.

Event ID: 516
Internal resources allocated for the queuing of security event messages have been exhausted, leading to the loss of some security event messages.

Event ID: 517
The audit log was cleared.
Event ID: 518
A notification package was loaded by the Security Accounts Manager.

Event ID: 519
A process is using an invalid local procedure call (LPC) port in an attempt to impersonate a client and reply or read from or write to a client address space.

Event ID: 520
The system time was changed.

*Note:* This audit normally appears twice.

### 7.3.1.3 Windows 2008 Security Events

#### Category: Account Logon

**Subcategory: Credential Validation**

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>4774</td>
<td>An account was mapped for logon.</td>
</tr>
<tr>
<td>4775</td>
<td>An account could not be mapped for logon.</td>
</tr>
<tr>
<td>4776</td>
<td>The domain controller attempted to validate the credentials for an account.</td>
</tr>
<tr>
<td>4777</td>
<td>The domain controller failed to validate the credentials for an account.</td>
</tr>
</tbody>
</table>

**Subcategory: Kerberos Service Ticket Operations**

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>4768</td>
<td>A Kerberos authentication ticket (TGT) was requested.</td>
</tr>
<tr>
<td>4769</td>
<td>A Kerberos service ticket was requested.</td>
</tr>
<tr>
<td>4770</td>
<td>A Kerberos service ticket was renewed.</td>
</tr>
<tr>
<td>4771</td>
<td>Kerberos pre-authentication failed.</td>
</tr>
<tr>
<td>4772</td>
<td>A Kerberos authentication ticket request failed.</td>
</tr>
</tbody>
</table>

#### Category: Account Management

**Subcategory: Application Group Management**

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>4783</td>
<td>A basic application group was created.</td>
</tr>
<tr>
<td>4784</td>
<td>A basic application group was changed.</td>
</tr>
<tr>
<td>4785</td>
<td>A member was added to a basic application group.</td>
</tr>
<tr>
<td>4786</td>
<td>A member was removed from a basic application group.</td>
</tr>
<tr>
<td>4787</td>
<td>A non-member was added to a basic application group.</td>
</tr>
<tr>
<td>4788</td>
<td>A non-member was removed from a basic application group.</td>
</tr>
<tr>
<td>4789</td>
<td>A basic application group was deleted.</td>
</tr>
<tr>
<td>4790</td>
<td>An LDAP query group was created.</td>
</tr>
</tbody>
</table>

**Subcategory: Computer Account Management**

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>4742</td>
<td>A computer account was changed.</td>
</tr>
<tr>
<td>4743</td>
<td>A computer account was deleted.</td>
</tr>
</tbody>
</table>

**Subcategory: Distribution Group Management**

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>4744</td>
<td>A security-disabled local group was created.</td>
</tr>
<tr>
<td>4745</td>
<td>A security-disabled local group was changed.</td>
</tr>
<tr>
<td>4746</td>
<td>A member was added to a security-disabled local group.</td>
</tr>
<tr>
<td>4747</td>
<td>A member was removed from a security-disabled local group.</td>
</tr>
</tbody>
</table>
4748 A security-disabled local group was deleted.
4749 A security-disabled global group was created.
4750 A security-disabled global group was changed.
4751 A member was added to a security-disabled global group.
4752 A member was removed from a security-disabled global group.
4753 A security-disabled global group was deleted.
4759 A security-disabled universal group was created.
4760 A security-disabled universal group was changed.
4761 A member was added to a security-disabled universal group.
4762 A member was removed from a security-disabled universal group.

Subcategory: Other Account Management Events
ID Message
4782 The password hash an account was accessed.
4793 The Password Policy Checking API was called.

Subcategory: Security Group Management
ID Message
4727 A security-enabled global group was created.
4728 A member was added to a security-enabled global group.
4729 A member was removed from a security-enabled global group.
4730 A security-enabled global group was deleted.
4731 A security-enabled local group was created.
4732 A member was added to a security-enabled local group.
4733 A member was removed from a security-enabled local group.
4734 A security-enabled local group was deleted.
4735 A security-enabled local group was changed.
4737 A security-enabled global group was changed.
4754 A security-enabled universal group was created.
4755 A security-enabled universal group was changed.
4756 A member was added to a security-enabled universal group.
4757 A member was removed from a security-enabled universal group.
4758 A security-enabled universal group was deleted.
4764 A group's type was changed.

Subcategory: User Account Management
ID Message
4720 A user account was created.
4722 A user account was enabled.
4723 An attempt was made to change an account's password.
4724 An attempt was made to reset an account's password.
4725 A user account was disabled.
4726 A user account was deleted.
4738 A user account was changed.
4740 A user account was locked out.
4765 SID History was added to an account.
4766 An attempt to add SID History to an account failed.
4767 A user account was unlocked.
4780 The ACL was set on accounts which are members of administrators groups.
4781 The name of an account was changed:
4794 An attempt was made to set the Directory Services Restore Mode.
5376 Credential Manager credentials were backed up.
5377 Credential Manager credentials were restored from a backup.

Category: Detailed Tracking
Subcategory: DPAPI Activity
ID    Message
4692  Backup of data protection master key was attempted.
4693  Recovery of data protection master key was attempted.
4694  Protection of auditable protected data was attempted.
4695  Unprotection of auditable protected data was attempted.

Subcategory: Process Creation
ID    Message
4688  A new process has been created.
4689  A process has exited.
4696  A primary token was assigned to process.

Subcategory: RPC Events
ID    Message
5712  A Remote Procedure Call (RPC) was attempted.

Category: DS Access

Subcategory: Detailed Directory Service Replication
ID    Message
4928  An Active Directory replica source naming context was established.
4929  An Active Directory replica source naming context was removed.
4930  An Active Directory replica source naming context was modified.
4931  An Active Directory replica destination naming context was modified.
4934  Attributes of an Active Directory object were replicated.
4935  Replication failure begins.
4936  Replication failure ends.
4937  A lingering object was removed from a replica.

Subcategory: Directory Service Access
ID    Message
4662  An operation was performed on an object.

Subcategory: Directory Service Changes
ID    Message
5136  A directory service object was modified.
5137  A directory service object was created.
5138  A directory service object was undeleted.
5139  A directory service object was moved.

Note: The following event in the Directory Service Changes subcategory is available only in Windows Vista Service Pack 1 and in Windows Server 2008.
ID    Message
5141  A directory service object was deleted.

Subcategory: Directory Service Replication
ID    Message
4932  Synchronization of a replica of an Active Directory naming context has begun.
4933  Synchronization of a replica of an Active Directory naming context has ended.

Category: Logon/Logoff
**Subcategory: IPsec Extended Mode**

- **ID 4978** During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
- **ID 4979** IPsec Main Mode and Extended Mode security associations were established.
- **ID 4980** IPsec Main Mode and Extended Mode security associations were established.
- **ID 4981** IPsec Main Mode and Extended Mode security associations were established.
- **ID 4982** IPsec Main Mode and Extended Mode security associations were established.
- **ID 4983** An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
- **ID 4984** An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

**Subcategory: IPsec Main Mode**

- **ID 4646** IKE DoS-prevention mode started.
- **ID 4650** An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
- **ID 4651** An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
- **ID 4652** An IPsec Main Mode negotiation failed.
- **ID 4653** An IPsec Main Mode negotiation failed.
- **ID 4655** An IPsec Main Mode security association ended.
- **ID 4976** During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
- **ID 5049** An IPsec Security Association was deleted.
- **ID 5453** An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.

**Subcategory: IPsec Quick Mode**

- **ID 4654** An IPsec Quick Mode negotiation failed.
- **ID 4977** During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
- **ID 5451** An IPsec Quick Mode security association was established.
- **ID 5452** An IPsec Quick Mode security association ended.

**Subcategory: Logoff**

- **ID 4634** An account was logged off.
- **ID 4647** User initiated logoff.

**Subcategory: Logon**

- **ID 4624** An account was successfully logged on.
- **ID 4625** An account failed to log on.
- **ID 4648** A logon was attempted using explicit credentials.
- **ID 4675** SIDs were filtered.

Note: All the events in the Network Policy Server subcategory are available only in Windows Vista Service Pack 1 and in Windows Server 2008.

**Subcategory: Network Policy Server**

- **ID 6272** Network Policy Server granted access to a user.
- **ID 6273** Network Policy Server denied access to a user.
- **ID 6274** Network Policy Server discarded the request for a user.
- **ID 6275** Network Policy Server discarded the accounting request for a user.
6276 Network Policy Server quarantined a user.
6277 Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
6278 Network Policy Server granted full access to a user because the host met the defined health policy.
6279 Network Policy Server locked the user account due to repeated failed authentication attempts.
6280 Network Policy Server unlocked the user account.

Subcategory: Other Logon/Logoff Events
ID   Message
4649 A replay attack was detected.
4778 A session was reconnected to a Window Station.
4779 A session was disconnected from a Window Station.
4800 The workstation was locked.
4801 The workstation was unlocked.
4802 The screen saver was invoked.
4803 The screen saver was dismissed.
5378 The requested credentials delegation was disallowed by policy.
5632 A request was made to authenticate to a wireless network.
5633 A request was made to authenticate to a wired network.

Subcategory: Special Logon
ID   Message
4964 Special groups have been assigned to a new logon.

Category: Object Access
Subcategory: Application Generated
ID   Message
4665 An attempt was made to create an application client context.
4666 An application attempted an operation:
4667 An application client context was deleted.
4668 An application was initialized.

Subcategory: Certification Services
ID   Message
4868 The certificate manager denied a pending certificate request.
4869 Certificate Services received a resubmitted certificate request.
4870 Certificate Services revoked a certificate.
4871 Certificate Services received a request to publish the certificate revocation list (CRL).
4872 Certificate Services published the certificate revocation list (CRL).
4873 A certificate request extension changed.
4874 One or more certificate request attributes changed.
4875 Certificate Services received a request to shut down.
4876 Certificate Services backup started.
4877 Certificate Services backup completed.
4878 Certificate Services restore started.
4879 Certificate Services restore completed.
4880 Certificate Services started.
4881 Certificate Services stopped.
4882 The security permissions for Certificate Services changed.
4883 Certificate Services retrieved an archived key.
4884 Certificate Services imported a certificate into its database.
4885 The audit filter for Certificate Services changed.
4886 Certificate Services received a certificate request.
4887 Certificate Services approved a certificate request and issued a certificate.
4888 Certificate Services denied a certificate request.
4889 Certificate Services set the status of a certificate request to pending.
4890 The certificate manager settings for Certificate Services changed.
4891 A configuration entry changed in Certificate Services.
4892 A property of Certificate Services changed.
4893 Certificate Services archived a key.
4894 Certificate Services imported and archived a key.
4895 Certificate Services published the CA certificate to Active Directory Domain Services.
4896 One or more rows have been deleted from the certificate database.
4897 Role separation enabled:
4898 Certificate Services loaded a template.

Subcategory: File Share
ID Message
5140 A network share object was accessed.

Subcategory: File System
ID Message
4664 An attempt was made to create a hard link.
4985 The state of a transaction has changed.
5051 A file was virtualized.

Subcategory: Filtering Platform Connection
ID Message
5031 The Windows Firewall Service blocked an application from accepting incoming connections on
the network.
5152 The Windows Filtering Platform blocked a packet.
5153 A more restrictive Windows Filtering Platform filter has blocked a packet.
5154 The Windows Filtering Platform has permitted an application or service to listen on a port for
incoming connections.
5155 The Windows Filtering Platform has blocked an application or service from listening on a port for
incoming connections.
5156 The Windows Filtering Platform has allowed a connection.
5157 The Windows Filtering Platform has blocked a connection.
5158 The Windows Filtering Platform has permitted a bind to a local port.
5159 The Windows Filtering Platform has blocked a bind to a local port.

Subcategory: Handle Manipulation
ID Message
4656 A handle to an object was requested.
4658 The handle to an object was closed.
4690 An attempt was made to duplicate a handle to an object.

Subcategory: Other Object Access Events
ID Message
4671 An application attempted to access a blocked ordinal through the TBS.
4691 Indirect access to an object was requested.
4698 A scheduled task was created.
4699 A scheduled task was deleted.
4700 A scheduled task was enabled.
4701 A scheduled task was disabled.
4702 A scheduled task was updated.
5888 An object in the COM+ Catalog was modified.
5889 An object was deleted from the COM+ Catalog.
5890 An object was added to the COM+ Catalog.
Subcategory: Registry
ID          Message
4657        A registry value was modified.
5039        A registry key was virtualized.

Subcategory: Subcategory
Note: The following event may be generated by any resource manager when enabling its subcategory. For example, the following event may be generated by the Registry resource manager or the File System resource manager.
ID          Message
4659        A handle to an object was requested with intent to delete.
4660        An object was deleted.
4661        A handle to an object was requested.
4663        An attempt was made to access an object.

Category: Policy Change

Subcategory: Audit Policy Change
ID          Message
4715        The audit policy (SACL) on an object was changed.
4719        System audit policy was changed.
4902        The Per-user audit policy table was created.
4904        An attempt was made to register a security event source.
4905        An attempt was made to unregister a security event source.
4906        The CrashOnAuditFail value has changed.
4907        Auditing settings on object were changed.
4908        Special Groups Logon table modified.
4912        Per User Audit Policy was changed.

Subcategory: Authentication Policy Change
ID          Message
4706        A new trust was created to a domain.
4707        A trust to a domain was removed.
4713        Kerberos policy was changed.
4716        Trusted domain information was modified.
4717        System security access was granted to an account.
4718        System security access was removed from an account.
4739        Domain Policy was changed.
4864        A namespace collision was detected.
4865        A trusted forest information entry was added.
4866        A trusted forest information entry was removed.
4867        A trusted forest information entry was modified.

Subcategory: Authorization Policy Change
ID          Message
4704        A user right was assigned.
4705        A user right was removed.
4714        Encrypted data recovery policy was changed.

Subcategory: Filtering Platform Policy Change
ID          Message
4709        IPsec Services was started.
4710        IPsec Services was disabled.
4711        May contain any one of the following:
• PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
• PAStore Engine applied Active Directory storage IPsec policy on the computer.
• PAStore Engine applied local registry storage IPsec policy on the computer.
• PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
• PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
• PAStore Engine failed to apply local registry storage IPsec policy on the computer.
• PAStore Engine failed to apply some rules of the active IPsec policy on the computer.
• PAStore Engine failed to load directory storage IPsec policy on the computer.
• PAStore Engine failed to load local storage IPsec policy on the computer.
• PAStore Engine loaded local storage IPsec policy on the computer.
• PAStore Engine polled for changes to the active IPsec policy and detected no changes.

4712 IPsec Services encountered a potentially serious failure.
5040 A change has been made to IPsec settings. An Authentication Set was added.
5041 A change has been made to IPsec settings. An Authentication Set was modified.
5042 A change has been made to IPsec settings. An Authentication Set was deleted.
5043 A change has been made to IPsec settings. A Connection Security Rule was added.
5044 A change has been made to IPsec settings. A Connection Security Rule was modified.
5045 A change has been made to IPsec settings. A Connection Security Rule was deleted.
5046 A change has been made to IPsec settings. A Crypto Set was added.
5047 A change has been made to IPsec settings. A Crypto Set was modified.
5048 A change has been made to IPsec settings. A Crypto Set was deleted.
5440 The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
5441 The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
5442 The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
5443 The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
5444 The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.
5446 A Windows Filtering Platform callout has been changed.
5448 A Windows Filtering Platform provider has been changed.
5449 A Windows Filtering Platform provider context has been changed.
5450 A Windows Filtering Platform sub-layer has been changed.
5456 PAStore Engine applied Active Directory storage IPsec policy on the computer.
5457 PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
5458 PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
5459 PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
5460 PAStore Engine applied local registry storage IPsec policy on the computer.
5461 PAStore Engine failed to apply local registry storage IPsec policy on the computer.
5462 PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.
5463 PAStore Engine polled for changes to the active IPsec policy and detected no changes.
5464 PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.
5465 PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.
5466 PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.
5467  PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.
5468  PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.
5471  PAStore Engine loaded local storage IPsec policy on the computer.
5472  PAStore Engine failed to load local storage IPsec policy on the computer.
5473  PAStore Engine loaded directory storage IPsec policy on the computer.
5474  PAStore Engine failed to load directory storage IPsec policy on the computer.
5477  PAStore Engine failed to add quick mode filter.

Subcategory: MPSSVC Rule-Level Policy Change
ID  Message
4944  The following policy was active when the Windows Firewall started.
4945  A rule was listed when the Windows Firewall started.
4946  A change has been made to Windows Firewall exception list. A rule was added.
4947  A change has been made to Windows Firewall exception list. A rule was modified.
4948  A change has been made to Windows Firewall exception list. A rule was deleted.
4949  Windows Firewall settings were restored to the default values.
4950  A Windows Firewall setting has changed.
4951  A rule has been ignored because its major version number was not recognized by Windows Firewall.
4952  Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
4953  A rule has been ignored by Windows Firewall because it could not parse the rule.
4954  Windows Firewall Group Policy settings have changed. The new settings have been applied.
4956  Windows Firewall has changed the active profile.
4957  Windows Firewall did not apply the following rule:
4958  Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:

Subcategory: Other Policy Change Events
ID  Message
4909  The local policy settings for the TBS were changed.
4910  The group policy settings for the TBS were changed.
5063  A cryptographic provider operation was attempted.
5064  A cryptographic context operation was attempted.
5065  A cryptographic context modification was attempted.
5066  A cryptographic function operation was attempted.
5067  A cryptographic function modification was attempted.
5068  A cryptographic function provider operation was attempted.
5069  A cryptographic function property operation was attempted.
5070  A cryptographic function property modification was attempted.
5447  A Windows Filtering Platform filter has been changed.
6144  Security policy in the group policy objects has been applied successfully.
6145  One or more errors occurred while processing security policy in the group policy objects.

Subcategory: Subcategory
Note The following event may be generated by any resource manager when enabling its subcategory. For example, the following event may be generated by the Registry resource manager or the File System resource manager.
ID  Message
4670  Permissions on an object were changed.
Category: Privilege Use

Subcategory: Sensitive Privilege Use / Non Sensitive Privilege Use

ID   Message
4672 Special privileges assigned to new logon.
4673 A privileged service was called.
4674 An operation was attempted on a privileged object.

Category: System

Subcategory: IPsec Driver

ID   Message
4960 IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
4961 IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
4962 IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.
4963 IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
4965 IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, these events can be ignored.
5478 IPsec Services has started successfully.
5479 IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5480 IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
5483 IPsec Services failed to initialize RPC server. IPsec Services could not be started.
5484 IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5485 IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

Subcategory: Other System Events

ID   Message
5024 The Windows Firewall Service has started successfully.
5025 The Windows Firewall Service has been stopped.
5027 The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
5028 The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
5029 The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
5030 The Windows Firewall Service failed to start.
5032  Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
5033  The Windows Firewall Driver has started successfully.
5034  The Windows Firewall Driver has been stopped.
5035  The Windows Firewall Driver failed to start.
5037  The Windows Firewall Driver detected critical runtime error. Terminating.
5058  Key file operation.
5059  Key migration operation.

Subcategory: Security State Change
ID  Message
4608  Windows is starting up.
4609  Windows is shutting down.
4616  The system time was changed.
4621  Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.

Subcategory: Security System Extension
ID  Message
4610  An authentication package has been loaded by the Local Security Authority.
4611  A trusted logon process has been registered with the Local Security Authority.
4614  A notification package has been loaded by the Security Account Manager.
4622  A security package has been loaded by the Local Security Authority.
4697  A service was installed in the system.

Subcategory: System Integrity
ID  Message
4612  Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
4615  Invalid use of LPC port.
4618  A monitored security event pattern has occurred.
4616  RPC detected an integrity violation while decrypting an incoming message.
5038  Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
5056  A cryptographic self test was performed.
5057  A cryptographic primitive operation failed.
5060  Verification operation failed.
5061  Cryptographic operation.
5062  A kernel-mode cryptographic self test was performed.

### 7.3.1.4 Windows 2012 Security Events

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Event ID</th>
<th>Message Summary</th>
<th>Minimum Operating System Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>4609</td>
<td>Windows is shutting down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security System Extension</td>
<td>4610</td>
<td>An authentication package has been loaded by the Local Security Authority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4611</td>
<td>A trusted logon process has been registered with the Local Security Authority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Integrity</td>
<td>4612</td>
<td>Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security System Extension</td>
<td>4614</td>
<td>A notification package has been loaded by the Security Account Manager.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Integrity</td>
<td>4615</td>
<td>Invalid use of LPC port.</td>
<td></td>
</tr>
<tr>
<td>Event Category</td>
<td>Event ID</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security State Change</td>
<td>4616</td>
<td>The system time was changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Integrity</td>
<td>4618</td>
<td>A monitored security event pattern has occurred.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security State Change</td>
<td>4621</td>
<td>Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security System Extension</td>
<td>4622</td>
<td>A security package has been loaded by the Local Security Authority.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon</td>
<td>4624</td>
<td>An account was successfully logged on.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4625</td>
<td>An account failed to log on.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logoff</td>
<td>4626</td>
<td>User/Device claims information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Membership</td>
<td>4627</td>
<td>Group membership information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon</td>
<td>4634</td>
<td>An account was logged off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec Main Mode</td>
<td>4646</td>
<td>An IPSec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logoff</td>
<td>4647</td>
<td>User initiated logoff.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon</td>
<td>4648</td>
<td>A logon was attempted using explicit credentials.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Logon/Logoff Events</td>
<td>4649</td>
<td>A replay attack was detected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec Main Mode</td>
<td>4650</td>
<td>An IPSec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4651</td>
<td>An IPSec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4652</td>
<td>An IPSec Main Mode negotiation failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4653</td>
<td>An IPSec Main Mode negotiation failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec Quick Mode</td>
<td>4654</td>
<td>An IPSec Quick Mode negotiation failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec Main Mode</td>
<td>4655</td>
<td>An IPSec Main Mode security association ended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handle Manipulation</td>
<td>4656</td>
<td>A handle to an object was requested.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry</td>
<td>4657</td>
<td>A registry value was modified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handle Manipulation</td>
<td>4658</td>
<td>The handle to an object was closed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAM</td>
<td>4659</td>
<td>A handle to an object was requested with intent to delete.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kernel</td>
<td>4659</td>
<td>A handle to an object was requested with intent to delete.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAM</td>
<td>4660</td>
<td>An object was deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kernel</td>
<td>4660</td>
<td>An object was deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAM</td>
<td>4661</td>
<td>A handle to an object was requested.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kernel</td>
<td>4661</td>
<td>A handle to an object was requested.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory Service Access</td>
<td>4662</td>
<td>An operation was performed on an object.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAM</td>
<td>4663</td>
<td>An attempt was made to access an object.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kernel</td>
<td>4663</td>
<td>An attempt was made to access an object.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File System</td>
<td>4664</td>
<td>An attempt was made to create a hard link.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Generated</td>
<td>4665</td>
<td>An attempt was made to create an application client context.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4666</td>
<td>An application attempted an operation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4667</td>
<td>An application client context was deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4668</td>
<td>An application was initialized.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subcategory (special)</td>
<td>4670</td>
<td>Permissions on an object were changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Object Access Events</td>
<td>4671</td>
<td>An application attempted to access a blocked ordinal through the TBS.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensitive Privilege Use / Non Sensitive Privilege Use</td>
<td>4672</td>
<td>Special privileges assigned to new logon.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>Event ID</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon/Logoff</td>
<td>Logon</td>
<td>SIDs were filtered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed Tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Creation</td>
<td>4675</td>
<td>A new process has been created.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Termination</td>
<td>4689</td>
<td>A process has exited.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handle Manipulation</td>
<td>4690</td>
<td>An attempt was made to duplicate a handle to an object.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Object Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>4691</td>
<td>Indirect access to an object was requested.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed Tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPAPI Activity</td>
<td>4692</td>
<td>Backup of data protection master key was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4693</td>
<td>Recovery of data protection master key was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4694</td>
<td>Protection of auditable protected data was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4695</td>
<td>Unprotection of auditable protected data was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Security System Extension</td>
<td>A service was installed in the system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Object Access</td>
<td>4696</td>
<td>A primary token was assigned to process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization Policy</td>
<td>4703</td>
<td>A user right was adjusted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>4704</td>
<td>A user right was assigned.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4705</td>
<td>A user right was removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4706</td>
<td>A new trust was created to a domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4707</td>
<td>A trust to a domain was removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filtering Platform</td>
<td>4709</td>
<td>IPsec Services was started.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4710</td>
<td>IPsec Services was disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>May contain any one of the following: PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine applied Active Directory storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine applied local registry storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine failed to apply local registry storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine failed to apply some rules of the active IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine failed to load directory storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine loaded directory storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine failed to load local storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine loaded local storage IPsec policy on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PAStore Engine polled for changes to the active IPsec policy and detected no changes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Policy</td>
<td>4712</td>
<td>IPsec Services encountered a potentially serious failure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization Policy</td>
<td>4713</td>
<td>Kerberos policy was changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>4714</td>
<td>Encrypted data recovery policy was changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Code</td>
<td>Event Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4715</td>
<td>The audit policy (SACL) on an object was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4716</td>
<td>Trusted domain information was modified.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4717</td>
<td>System security access was granted to an account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4718</td>
<td>System security access was removed from an account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4719</td>
<td>System audit policy was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4720</td>
<td>A user account was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4721</td>
<td>A user account was enabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4722</td>
<td>An attempt was made to change an account's password.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4723</td>
<td>An attempt was made to reset an account's password.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4724</td>
<td>A user account was disabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4725</td>
<td>A user account was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4727</td>
<td>A security-enabled global group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4728</td>
<td>A member was added to a security-enabled global group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4729</td>
<td>A member was removed from a security-enabled global group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4730</td>
<td>A security-enabled global group was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4731</td>
<td>A security-enabled local group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a security-enabled local group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4733</td>
<td>A member was removed from a security-enabled local group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4734</td>
<td>A security-enabled local group was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4735</td>
<td>A security-enabled local group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4736</td>
<td>A security-enabled global group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4737</td>
<td>A user account was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4738</td>
<td>A domain policy was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4740</td>
<td>A user account was locked out.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4742</td>
<td>A computer account was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4743</td>
<td>A computer account was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4744</td>
<td>A security-disabled local group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4745</td>
<td>A security-disabled local group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4746</td>
<td>A member was added to a security-disabled local group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4747</td>
<td>A member was removed from a security-disabled local group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4748</td>
<td>A security-disabled local group was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4749</td>
<td>A security-disabled global group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4750</td>
<td>A security-disabled global group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4751</td>
<td>A member was added to a security-disabled global group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4752</td>
<td>A member was removed from a security-disabled global group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4753</td>
<td>A security-disabled global group was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4754</td>
<td>A security-disabled universal group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4755</td>
<td>A security-disabled universal group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4756</td>
<td>A member was added to a security-disabled universal group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4757</td>
<td>A member was removed from a security-disabled universal group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4758</td>
<td>A security-disabled universal group was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4759</td>
<td>A security-disabled universal group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4760</td>
<td>A security-disabled universal group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4761</td>
<td>A member was added to a security-disabled universal group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4762</td>
<td>A member was removed from a security-disabled universal group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4764</td>
<td>A group's type was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4765</td>
<td>SID History was added to an account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4766</td>
<td>An attempt to add SID History to an account failed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4767</td>
<td>A user account was unlocked.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4768</td>
<td>A security-disabled universal group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4768</td>
<td>A Kerberos authentication ticket (TGT) was requested.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4769</td>
<td>A Kerberos service ticket was requested.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4770</td>
<td>A Kerberos service ticket was renewed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4771</td>
<td>Kerberos pre-authentication failed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4772</td>
<td>A Kerberos authentication ticket request failed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4773</td>
<td>A Kerberos service ticket request failed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4774</td>
<td>An account was mapped for logon.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4775</td>
<td>An account could not be mapped for logon.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4776</td>
<td>The domain controller attempted to validate the credentials for an account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4777</td>
<td>The domain controller failed to validate the credentials for an account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4778</td>
<td>A session was reconnected to a Window Station.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4779</td>
<td>A session was disconnected from a Window Station.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4780</td>
<td>The ACL was set on accounts which are members of administrators groups.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4781</td>
<td>The name of an account was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4782</td>
<td>The password hash an account was accessed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4783</td>
<td>A basic application group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4784</td>
<td>A basic application group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4785</td>
<td>A member was added to a basic application group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4786</td>
<td>A member was removed from a basic application group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4787</td>
<td>A non-member was added to a basic application group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4788</td>
<td>A non-member was removed from a basic application group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4789</td>
<td>A basic application group was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4790</td>
<td>An LDAP query group was created.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4791</td>
<td>A basic application group was changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4792</td>
<td>An LDAP query group was deleted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4793</td>
<td>The Password Policy Checking API was called.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4794</td>
<td>An attempt was made to set the Directory Services Restore Mode.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4795</td>
<td>An attempt was made to query the existence of a blank password for an account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4796</td>
<td>A user's local group membership was enumerated.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4799</td>
<td>A security-enabled local group membership was enumerated.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4800</td>
<td>The workstation was locked.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4801</td>
<td>The workstation was unlocked.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4802</td>
<td>The screen saver was invoked.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4803</td>
<td>The screen saver was dismissed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4816</td>
<td>RPC detected an integrity violation while decrypting an incoming message.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4817</td>
<td>Auditing settings on an object were changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4818</td>
<td>Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4819</td>
<td>Central Access Policies on the machine have been changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4820</td>
<td>A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerberos Service Ticket Operations</td>
<td>4821</td>
<td>A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.</td>
<td>Windows 8.1, Windows Server 2012 R2</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Credential Validation</td>
<td>4822</td>
<td>NTLM authentication failed because the account was a member of the Protected User group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4823</td>
<td>NTLM authentication failed because access control restrictions are required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerberos Authentication Service</td>
<td>4824</td>
<td>Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon/Logoff</td>
<td>4825</td>
<td>A user was denied the access to Remote Desktop.</td>
<td>Windows Vista SP2, Windows Server 2008 SP2</td>
<td></td>
</tr>
<tr>
<td>Other Logon/Logoff Events</td>
<td>4826</td>
<td>Boot Configuration Data loaded.</td>
<td>Windows 10</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>4864</td>
<td>A namespace collision was detected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Policy Change</td>
<td>4865</td>
<td>A trusted forest information entry was added.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4866</td>
<td>A trusted forest information entry was removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4867</td>
<td>A trusted forest information entry was modified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4868</td>
<td>The certificate manager denied a pending certificate request.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4869</td>
<td>Certificate Services received a resubmitted certificate request.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4870</td>
<td>Certificate Services revoked a certificate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4871</td>
<td>Certificate Services received a request to publish the certificate revocation list (CRL).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4872</td>
<td>Certificate Services published the certificate revocation list (CRL).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4873</td>
<td>A certificate request extension changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4874</td>
<td>One or more certificate request attributes changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4875</td>
<td>Certificate Services received a request to shut down.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4876</td>
<td>Certificate Services backup started.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4877</td>
<td>Certificate Services backup completed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4878</td>
<td>Certificate Services restore started.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4879</td>
<td>Certificate Services restore completed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4880</td>
<td>Certificate Services started.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4881</td>
<td>Certificate Services stopped.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4883</td>
<td>Certificate Services retrieved an archived key.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4884</td>
<td>Certificate Services imported a certificate into its database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4885</td>
<td>The audit filter for Certificate Services changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4886</td>
<td>Certificate Services received a certificate request.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4887</td>
<td>Certificate Services approved a certificate request and issued a certificate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4888</td>
<td>Certificate Services denied a certificate request.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4889</td>
<td>Certificate Services set the status of a certificate request to pending.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4890</td>
<td>The certificate manager settings for Certificate Services changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4891</td>
<td>A configuration entry changed in Certificate Services.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4892</td>
<td>A property of Certificate Services changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4893</td>
<td>Certificate Services archived a key.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4894</td>
<td>Certificate Services imported and archived a key.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4895</td>
<td>Certificate Services published the CA certificate to Active Directory Domain Services.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4896</td>
<td>One or more rows have been deleted from the certificate database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4897</td>
<td>Role separation enabled:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4898</td>
<td>Certificate Services loaded a template.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4899</td>
<td>A Certificate Services template was updated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Policy Change</td>
<td>4900</td>
<td>Certificate Services template security was updated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4902</td>
<td>The Per-user audit policy table was created.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4904</td>
<td>An attempt was made to register a security event source.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4905</td>
<td>An attempt was made to unregister a security event source.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4906</td>
<td>The CrashOnAuditFail value has changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4907</td>
<td>Auditing settings on object were changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4908</td>
<td>Special Groups Logon table modified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Policy Change Events</td>
<td>4909</td>
<td>The local policy settings for the TBS were changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization Policy Change</td>
<td>4911</td>
<td>Resource attributes of the object were changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Policy Change</td>
<td>4912</td>
<td>Per User Audit Policy was changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization Policy Change</td>
<td>4913</td>
<td>Central Access Policy on the object was changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed Directory Service Replication</td>
<td>4928</td>
<td>An Active Directory replica source naming context was established.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4929</td>
<td>An Active Directory replica source naming context was removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4930</td>
<td>An Active Directory replica source naming context was modified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4931</td>
<td>An Active Directory replica destination naming context was modified.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory Service Replication</td>
<td>4932</td>
<td>Synchronization of a replica of an Active Directory naming context has begun.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4933</td>
<td>Synchronization of a replica of an Active Directory naming context has ended.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed Directory Service Replication</td>
<td>4934</td>
<td>Attributes of an Active Directory object were replicated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4935</td>
<td>Replication failure begins.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4936</td>
<td>Replication failure ends.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4937</td>
<td>A lingering object was removed from a replica.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPSSVC Rule-Level Policy Change</td>
<td>4944</td>
<td>The following policy was active when the Windows Firewall all started.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4945</td>
<td>A rule was listed when the Windows Firewall all started.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4946</td>
<td>A change has been made to Windows Firewall all exception list. A rule was added.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4947</td>
<td>A change has been made to Windows Firewall all exception list. A rule was modified.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4948</td>
<td>A change has been made to Windows Firewall all exception list. A rule was deleted.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4949</td>
<td>Windows Firewall all settings were restored to the default values.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4950</td>
<td>A Windows Firewall all setting has changed.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4951</td>
<td>A rule has been ignored because its major version number was not recognized by Windows Firewall.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4952</td>
<td>Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4953</td>
<td>A rule has been ignored by Windows Firewall all because it could not parse the rule.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4954</td>
<td>Windows Firewall all Group Policy settings have changed. The new settings have been applied.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4955</td>
<td>Windows Firewall all has changed the active profile.</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4956</td>
<td>Windows Firewall all did not apply the following rule:</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>4957</td>
<td>Windows Firewall all did not apply the following rule because the rule referred to items not configured on this computer:</td>
<td></td>
<td>Windows Vista, Windows Server 2008</td>
</tr>
<tr>
<td>System</td>
<td>4960</td>
<td>IpSec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4961</td>
<td>System</td>
<td>IPSec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4962</td>
<td>System</td>
<td>IPSec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4963</td>
<td>System</td>
<td>IPSec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPSec policy without informing this computer. This could also be a spoofing attack attempt.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4964</td>
<td>System</td>
<td>Special groups have been assigned to a new logon.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4965</td>
<td>System</td>
<td>IPSec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPSec implementations. In that case, if connectivity is not impeded, then these events can be ignored.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4966</td>
<td>System</td>
<td>During Main Mode negotiation, IPSec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4967</td>
<td>System</td>
<td>During Quick Mode negotiation, IPSec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4968</td>
<td>System</td>
<td>During Extended Mode negotiation, IPSec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4969</td>
<td>System</td>
<td>IPSec Main Mode and Extended Mode security associations were established.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4970</td>
<td>System</td>
<td>IPSec Main Mode and Extended Mode security associations were established.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4971</td>
<td>System</td>
<td>IPSec Main Mode and Extended Mode security associations were established.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4972</td>
<td>System</td>
<td>IPSec Main Mode and Extended Mode security associations were established.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4973</td>
<td>System</td>
<td>An IPSec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4974</td>
<td>System</td>
<td>An IPSec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4985</td>
<td>Object Access</td>
<td>The state of a transaction has changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5024</td>
<td>System</td>
<td>The Windows Firewall Service has started successfully.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5025</td>
<td>System</td>
<td>The Windows Firewall Service has been stopped.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5026</td>
<td>System</td>
<td>The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5027</td>
<td>System</td>
<td>The Windows Firewall Service was unable to parse the new security policy. The service will continue with the currently enforced policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5028</td>
<td>System</td>
<td>The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5029</td>
<td>System</td>
<td>The Windows Firewall Service failed to start.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5030</td>
<td>System</td>
<td>The Windows Firewall Service blocked an application from accepting incoming connections on the network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Events</td>
<td>Event ID</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5032</td>
<td>Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5033</td>
<td>The Windows Firewall Driver has started successfully.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5034</td>
<td>The Windows Firewall Driver has been stopped.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5035</td>
<td>The Windows Firewall Driver failed to start.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5037</td>
<td>The Windows Firewall Driver detected critical runtime error. Terminating.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Integrity</td>
<td>5038</td>
<td>Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td>Registry</td>
<td>5039</td>
<td>A registry key was virtualized.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5040</td>
<td>A change has been made to IPsec settings. An Authentication Set was added.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5041</td>
<td>A change has been made to IPsec settings. An Authentication Set was modified.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5042</td>
<td>A change has been made to IPsec settings. An Authentication Set was deleted.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5043</td>
<td>A change has been made to IPsec settings. A Connection Security Rule was added.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5044</td>
<td>A change has been made to IPsec settings. A Connection Security Rule was modified.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5045</td>
<td>A change has been made to IPsec settings. A Connection Security Rule was deleted.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5046</td>
<td>A change has been made to IPsec settings. A Crypto Set was added.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5047</td>
<td>A change has been made to IPsec settings. A Crypto Set was modified.</td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>Filter</td>
<td>5048</td>
<td>A change has been made to IPsec settings. A Crypto Set was deleted.</td>
<td></td>
</tr>
<tr>
<td>Logon/Logoff</td>
<td>IPSec Main Mode</td>
<td>5049</td>
<td>An IPsec Security Association was deleted.</td>
<td></td>
</tr>
<tr>
<td>System Events</td>
<td>Other System Events</td>
<td>5050</td>
<td>An attempt to programmatically disable the Windows Firewall was rejected because this API is not supported on Windows Vista.</td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td>File System</td>
<td>5051</td>
<td>A file was virtualized.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>System Integrity</td>
<td>5056</td>
<td>A cryptographic self test was performed.</td>
<td></td>
</tr>
<tr>
<td>System Events</td>
<td>Other System Events</td>
<td>5057</td>
<td>A cryptographic primitive operation failed.</td>
<td></td>
</tr>
<tr>
<td>System Integrity</td>
<td>Key file operation.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Events</td>
<td>Key migration operation.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Integrity</td>
<td>Verification operation failed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Bedrooms</td>
<td>Cryptographic operation.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5062</td>
<td>A kernel-mode cryptographic self test was performed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5063</td>
<td>A cryptographic provider operation was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5064</td>
<td>A cryptographic context operation was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5065</td>
<td>A cryptographic context modification was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5066</td>
<td>A cryptographic function operation was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5067</td>
<td>A cryptographic function modification was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5068</td>
<td>A cryptographic function provider operation was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5069</td>
<td>A cryptographic function property operation was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Change</td>
<td>5070</td>
<td>A cryptographic function property modification was attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Events</td>
<td>Other System Events</td>
<td>5071</td>
<td>Key access denied by Microsoft key distribution service.</td>
<td></td>
</tr>
<tr>
<td>Windows 8, Windows Server 2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td>Certification Services</td>
<td>5120</td>
<td>OCSP Responder Service Started.</td>
<td></td>
</tr>
<tr>
<td>Windows Vista, Windows Server 2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td>Certification Services</td>
<td>5121</td>
<td>OCSP Responder Service Stopped.</td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td>Certification Services</td>
<td>5122</td>
<td>A Configuration entry changed in the OCSP Responder Service.</td>
<td></td>
</tr>
<tr>
<td>TimeStamp</td>
<td>Event Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5123</td>
<td>A configuration entry changed in the OCSP Responder Service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5124</td>
<td>A security setting was updated on OCSP Responder Service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5125</td>
<td>A request was submitted to OCSP Responder Service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5126</td>
<td>Signing Certificate was automatically updated by the OCSP Responder Service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The OCSP Revocation Provider successfully updated the revocation information.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Directory Service Changes**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5136</td>
<td>A directory service object was modified.</td>
</tr>
<tr>
<td>5137</td>
<td>A directory service object was created.</td>
</tr>
<tr>
<td>5138</td>
<td>A directory service object was undeleted.</td>
</tr>
<tr>
<td>5139</td>
<td>A directory service object was moved.</td>
</tr>
</tbody>
</table>

**Object Access**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5140</td>
<td>A network share object was accessed.</td>
</tr>
</tbody>
</table>

**File Share**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5141</td>
<td>A directory service object was deleted.</td>
</tr>
</tbody>
</table>

**DS Access**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5142</td>
<td>A network share object was added.</td>
</tr>
<tr>
<td>5143</td>
<td>A network share object was modified.</td>
</tr>
<tr>
<td>5144</td>
<td>A network share object was deleted.</td>
</tr>
</tbody>
</table>

**Detailed File Share**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5145</td>
<td>A network share object was checked to see whether the client can be granted desired access.</td>
</tr>
</tbody>
</table>

**Filtering Platform Packet Drop**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5146</td>
<td>The Windows Filtering Platform has blocked a packet.</td>
</tr>
<tr>
<td>5147</td>
<td>A more restrictive Windows Filtering Platform filter has blocked a packet.</td>
</tr>
</tbody>
</table>

**Other Object Access Events**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5148</td>
<td>The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.</td>
</tr>
<tr>
<td>5149</td>
<td>The DoS attack has subsided and normal processing is being resumed.</td>
</tr>
</tbody>
</table>

**Filtering Platform Connection**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5150</td>
<td>The Windows Filtering Platform has blocked a packet.</td>
</tr>
<tr>
<td>5151</td>
<td>A more restrictive Windows Filtering Platform filter has blocked a packet.</td>
</tr>
</tbody>
</table>

**Filtering Platform Packet Drop**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5152</td>
<td>The Windows Filtering Platform blocked a packet.</td>
</tr>
<tr>
<td>5153</td>
<td>A more restrictive Windows Filtering Platform filter has blocked a packet.</td>
</tr>
</tbody>
</table>

**Filtering Platform Connection**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5154</td>
<td>The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.</td>
</tr>
<tr>
<td>5155</td>
<td>The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.</td>
</tr>
<tr>
<td>5156</td>
<td>The Windows Filtering Platform has allowed a connection.</td>
</tr>
<tr>
<td>5157</td>
<td>The Windows Filtering Platform has blocked a connection.</td>
</tr>
<tr>
<td>5158</td>
<td>The Windows Filtering Platform has permitted a bind to a local port.</td>
</tr>
<tr>
<td>5159</td>
<td>The Windows Filtering Platform has blocked a bind to a local port.</td>
</tr>
</tbody>
</table>

**File Share**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5168</td>
<td>Spn check for SMB/SMB2 failed.</td>
</tr>
</tbody>
</table>

**DS Access**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5169</td>
<td>A directory service object was modified.</td>
</tr>
</tbody>
</table>

**Account Management**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5376</td>
<td>Credential Manager credentials were backed up.</td>
</tr>
<tr>
<td>5377</td>
<td>Credential Manager credentials were restored from a backup.</td>
</tr>
</tbody>
</table>

**Logon/Logoff Events**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5378</td>
<td>The requested credentials delegation was disallowed by policy.</td>
</tr>
</tbody>
</table>

**Policy Change**

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5440</td>
<td>The following callout was present when the Windows Filtering Platform Base Filtering Engine started.</td>
</tr>
<tr>
<td>5441</td>
<td>The following filter was present when the Windows Filtering Platform Base Filtering Engine started.</td>
</tr>
</tbody>
</table>

© <2002 - 2022> ... NETIKUS.NET ltd
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5442</td>
<td>The following provider was present when the Windows Filtering Platform Base Filtering Engine started.</td>
</tr>
<tr>
<td>5443</td>
<td>The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.</td>
</tr>
<tr>
<td>5444</td>
<td>The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.</td>
</tr>
<tr>
<td>5446</td>
<td>A Windows Filtering Platform callout has been changed.</td>
</tr>
<tr>
<td>5447</td>
<td>A Windows Filtering Platform filter has been changed.</td>
</tr>
<tr>
<td>5448</td>
<td>A Windows Filtering Platform provider has been changed.</td>
</tr>
<tr>
<td>5449</td>
<td>A Windows Filtering Platform provider context has been changed.</td>
</tr>
<tr>
<td>5450</td>
<td>A Windows Filtering Platform sub-layer has been changed.</td>
</tr>
<tr>
<td>5451</td>
<td>A Windows Filtering Platform filter has been changed.</td>
</tr>
<tr>
<td>5452</td>
<td>A Windows Filtering Platform provider has been changed.</td>
</tr>
<tr>
<td>5453</td>
<td>A Windows Filtering Platform provider context has been changed.</td>
</tr>
<tr>
<td>5454</td>
<td>A Windows Filtering Platform sub-layer has been changed.</td>
</tr>
<tr>
<td>5455</td>
<td>A Windows Filtering Platform callout has been changed.</td>
</tr>
<tr>
<td>5456</td>
<td>A Windows Filtering Platform filter has been changed.</td>
</tr>
<tr>
<td>5457</td>
<td>A Windows Filtering Platform provider has been changed.</td>
</tr>
<tr>
<td>5458</td>
<td>A Windows Filtering Platform provider context has been changed.</td>
</tr>
<tr>
<td>5459</td>
<td>A Windows Filtering Platform sub-layer has been changed.</td>
</tr>
<tr>
<td>5460</td>
<td>A Windows Filtering Platform callout has been changed.</td>
</tr>
<tr>
<td>5461</td>
<td>A Windows Filtering Platform filter has been changed.</td>
</tr>
<tr>
<td>5462</td>
<td>A Windows Filtering Platform provider has been changed.</td>
</tr>
<tr>
<td>5463</td>
<td>A Windows Filtering Platform provider context has been changed.</td>
</tr>
<tr>
<td>5464</td>
<td>A Windows Filtering Platform sub-layer has been changed.</td>
</tr>
<tr>
<td>5465</td>
<td>A Windows Filtering Platform callout has been changed.</td>
</tr>
<tr>
<td>5466</td>
<td>A Windows Filtering Platform filter has been changed.</td>
</tr>
<tr>
<td>5467</td>
<td>A Windows Filtering Platform provider has been changed.</td>
</tr>
<tr>
<td>5468</td>
<td>A Windows Filtering Platform provider context has been changed.</td>
</tr>
<tr>
<td>5469</td>
<td>A Windows Filtering Platform sub-layer has been changed.</td>
</tr>
<tr>
<td>5470</td>
<td>A Windows Filtering Platform callout has been changed.</td>
</tr>
<tr>
<td>5471</td>
<td>A Windows Filtering Platform filter has been changed.</td>
</tr>
<tr>
<td>5472</td>
<td>A Windows Filtering Platform provider has been changed.</td>
</tr>
<tr>
<td>5473</td>
<td>A Windows Filtering Platform provider context has been changed.</td>
</tr>
<tr>
<td>5474</td>
<td>A Windows Filtering Platform sub-layer has been changed.</td>
</tr>
</tbody>
</table>

**Logon/Logoff**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5451</td>
<td>An IPsec Quick Mode security association was established.</td>
</tr>
<tr>
<td>5452</td>
<td>An IPsec Quick Mode security association ended.</td>
</tr>
<tr>
<td>5453</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
</tbody>
</table>

**Policy Change**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5453</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5454</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5455</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5456</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5457</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5458</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5459</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5460</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5461</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5462</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5463</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5464</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5465</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5466</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5467</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5468</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5469</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5470</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5471</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5472</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
<tr>
<td>5473</td>
<td>An IPsec negotiation with a remote computer failed because the IKE and AuthIP/IPsec Keying Modules (IKEEXT) service is not started.</td>
</tr>
</tbody>
</table>

© 2002 - 2022 NETIKUS.NET ltd
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5474</td>
<td>PAStore Engine failed to load directory storage IPsec policy on the computer.</td>
</tr>
<tr>
<td>5477</td>
<td>PAStore Engine failed to add quick mode filter.</td>
</tr>
<tr>
<td>5478</td>
<td>IPsec Services has started successfully.</td>
</tr>
<tr>
<td>5479</td>
<td>IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.</td>
</tr>
<tr>
<td>5480</td>
<td>IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.</td>
</tr>
<tr>
<td>5483</td>
<td>IPsec Services failed to initialize RPC server. IPsec Services could not be started.</td>
</tr>
<tr>
<td>5484</td>
<td>IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.</td>
</tr>
<tr>
<td>5485</td>
<td>IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.</td>
</tr>
<tr>
<td>5632</td>
<td>A request was made to authenticate to a wireless network.</td>
</tr>
<tr>
<td>5633</td>
<td>A request was made to authenticate to a wired network.</td>
</tr>
<tr>
<td>5712</td>
<td>A Remote Procedure Call (RPC) was attempted.</td>
</tr>
<tr>
<td>5888</td>
<td>An object in the COM+ Catalog was modified.</td>
</tr>
<tr>
<td>5889</td>
<td>An object was deleted from the COM+ Catalog.</td>
</tr>
<tr>
<td>5890</td>
<td>An object was added to the COM+ Catalog.</td>
</tr>
<tr>
<td>6144</td>
<td>Security policy in the group policy objects has been applied successfully.</td>
</tr>
<tr>
<td>6145</td>
<td>One or more errors occurred while processing security policy in the group policy objects.</td>
</tr>
<tr>
<td>6272</td>
<td>Network Policy Server granted access to a user.</td>
</tr>
<tr>
<td>6273</td>
<td>Network Policy Server denied access to a user.</td>
</tr>
<tr>
<td>6274</td>
<td>Network Policy Server discarded the request for a user.</td>
</tr>
<tr>
<td>6275</td>
<td>Network Policy Server discarded the accounting request for a user.</td>
</tr>
<tr>
<td>6276</td>
<td>Network Policy Server quarantined a user.</td>
</tr>
<tr>
<td>6277</td>
<td>Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.</td>
</tr>
<tr>
<td>6278</td>
<td>Network Policy Server granted full access to a user because the host met the defined health policy.</td>
</tr>
<tr>
<td>6279</td>
<td>Network Policy Server locked the user account due to repeated failed authentication attempts.</td>
</tr>
<tr>
<td>6280</td>
<td>Network Policy Server unlocked the user account.</td>
</tr>
<tr>
<td>6281</td>
<td>Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.</td>
</tr>
<tr>
<td>6400</td>
<td>BranchCache: Received an incorrectly formatted response while discovering availability of content.</td>
</tr>
<tr>
<td>6401</td>
<td>BranchCache: Received invalid data from a peer. Data discarded.</td>
</tr>
</tbody>
</table>
### Common Events

The following chapters list common event records that we collected from live systems in the field. It lists events from various types, both informational and critical. This list is neither complete nor to be used as a reference but instead can be used to get an idea of what types of events are logged to event logs.

Please send “interesting” events to support@netikus.net so that they can be included in this list, thank you.

1. Active Directory / DNS / WINS
2. System Events
3. Security
4. IIS / MSSQL / Exchange
5. Application Management
6. Hardware
### 7.3.2.1 Active Directory / DNS / WINS

These events are logged by Active Directory / DNS / WINS and indicate status information, errors or problems with the DNS or Active Directory.

<table>
<thead>
<tr>
<th>Event Log ID</th>
<th>Type</th>
<th>Source</th>
<th>Category</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server</td>
<td>400</td>
<td>Error</td>
<td>DNS</td>
<td>The DNS server was unable to open zone myzone.mydomain.com in the Active Directory. This DNS Server is configured to obtain and use information from the directory for this zone and is unable to load the zone without it. Check that the Active Directory is functioning properly and reload the zone. The event data is the error code.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>999</td>
<td>Warning</td>
<td>DNS</td>
<td>The DNS server has encountered numerous run-time events. These are usually caused by the reception of bad or unexpected packets, or from problems with or excessive replication traffic. The data is the number of suppressed events encountered in the last 15 minute interval.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>550</td>
<td>Warning</td>
<td>DNS</td>
<td>The DNS server encountered an invalid domain name in a packet from 12.23.34.23. The packet is rejected.</td>
</tr>
<tr>
<td>Application</td>
<td>100</td>
<td>Information</td>
<td>ESE</td>
<td>General</td>
</tr>
<tr>
<td>Application</td>
<td>300</td>
<td>Information</td>
<td>ESEN T</td>
<td>Logging/Recovery</td>
</tr>
<tr>
<td>Application</td>
<td>302</td>
<td>Information</td>
<td>ESEN T</td>
<td>Logging/Recovery</td>
</tr>
</tbody>
</table>

*Strings in italic may vary depending on what triggered the event*
### System Events

These events are logged by the Operating System and mostly indicate errors or problems with the system. Please note that even critical messages might just be logged as **Information** events.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Source</th>
<th>Category</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>System 16</td>
<td>Warning</td>
<td>Automatic Updates</td>
<td>Download</td>
</tr>
<tr>
<td>System 6005</td>
<td>Information</td>
<td>EventLog</td>
<td></td>
</tr>
<tr>
<td>System 6006</td>
<td>Information</td>
<td>EventLog</td>
<td></td>
</tr>
<tr>
<td>System 6009</td>
<td>Error</td>
<td>EventLog</td>
<td></td>
</tr>
<tr>
<td>System 6009</td>
<td>Information</td>
<td>EventLog</td>
<td></td>
</tr>
<tr>
<td>System 1073</td>
<td>Warning</td>
<td>USER32</td>
<td></td>
</tr>
<tr>
<td>System 2923</td>
<td>Information</td>
<td>LSASRV</td>
<td></td>
</tr>
<tr>
<td>System 4096 0</td>
<td>Warning</td>
<td>LSASRV</td>
<td>SPNEGO (Negotiator)</td>
</tr>
<tr>
<td>System 4096 1</td>
<td>Warning</td>
<td>LSASRV</td>
<td>SPNEGO (Negotiator)</td>
</tr>
<tr>
<td>System 3034</td>
<td>Warning</td>
<td>MRxSmb</td>
<td></td>
</tr>
<tr>
<td>System 3019</td>
<td>Warning</td>
<td>MRxSmb</td>
<td></td>
</tr>
<tr>
<td>System 2511</td>
<td>Error</td>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>System 2506</td>
<td>Error</td>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>System 2012</td>
<td>Error</td>
<td>Srv</td>
<td></td>
</tr>
<tr>
<td>System 1665 0</td>
<td>Error</td>
<td>SAM</td>
<td></td>
</tr>
</tbody>
</table>
Controller. Please look for other SAM event logs that may indicate the exact reason for the failure.

System 64 Warning w32time
Because of repeated network problems, the time service has not been able to find a domain controller to synchronize with for a long time. To reduce network traffic, the time service will wait 960 minutes before trying again. No synchronization will take place during this interval, even if network connectivity is restored. Accumulated time errors may cause certain network operations to fail. To tell the time service that network connectivity has been restored and that it should resynchronize, execute "w32tm /s" from the command line.

System 54 Warning w32time
The Windows Time Service was not able to find a Domain Controller. A time and date update was not possible.

System 24 Warning w32time
Time Provider NtpClient: No valid response has been received from domain controller mydc.mydomain.com after 8 attempts to contact it. This domain controller will be discarded as a time source and NtpClient will attempt to discover a new domain controller from which to synchronize.

System 2005 Error RemoteAccess
The user DOMAIN\Ingmar connected to port VPN2-120 has been disconnected because no network protocols were successfully negotiated.

System 2018 Warning RemoteAccess
The user Intruder connected from 12.23.34.55 but failed an authentication attempt due to the following reason: (4112).

System 1001 Information Save Dump
The computer has rebooted from a bugcheck. The bugcheck was: 0x000000d1 (0x00000002 0x00000009 0x000000 xf1c21934). Microsoft Windows 2000 [v15.2195]. A dump was saved in: C:\WINNT\MEMORY.DMP.

System 1003 Warning Dhcp
Your computer was not able to renew its address from the network (from the DHCP Server) for the Network Card with network address 00053C08910F. The following error occurred: The operation was canceled by the user. Your computer will continue to try and obtain an address on its own from the network address (DHCP) server.

Strings in italic may vary depending on what triggered the event
7.3.2.3 Security

These events are logged by the security sub-system of Windows. For a complete list of possible events see "Windows 2000 Security Event Descriptions".

<table>
<thead>
<tr>
<th>Event Log</th>
<th>ID</th>
<th>Type</th>
<th>Source</th>
<th>Category</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>59</td>
<td>Audit</td>
<td>Security</td>
<td>Detailed Tracking</td>
<td>Backup of data protection master key. Key Identifier: 38b2f717-214b-4c2a-00e0-0ee945fa4616 Recovery Server: Recovery Key ID: Failure Reason: 0x32</td>
</tr>
<tr>
<td>Security</td>
<td>61</td>
<td>Audit</td>
<td>Security</td>
<td>Policy Change</td>
<td>IPSec Services: IPSec Services failed to get the complete list of network interfaces on the machine. This can be a potential security hazard to the machine since some of the network interfaces may not get the protection as desired by the applied IPSec filters. Please run IPSec monitor snap-in to further diagnose the problem.</td>
</tr>
<tr>
<td>Security</td>
<td>61</td>
<td>Audit</td>
<td>Security</td>
<td>Policy Change</td>
<td>Audit Policy Change: New Policy: Success Failure + + Logon/Logoff + + Object Access - + Privilege Use + + Account Management + + Policy Change + + System - + Detailed Tracking + + Directory Service Access + + Account Logon Changed By: User Name: SHEEP$ Domain Name: NETIKUS Logon ID: (0x0,0x3E7)</td>
</tr>
<tr>
<td>Security</td>
<td>62</td>
<td>Audit</td>
<td>Security</td>
<td>Account Management</td>
<td>Change Password Attempt: Target Account Name: Administrator Target Domain: SHEEP Target Account ID: SHEEP\Administrator Caller User Name: SHEEP$ Caller Domain: NETIKUS Caller Logon ID: (0x0,0x3E7) Privileges: -</td>
</tr>
</tbody>
</table>

Strings in italic may vary depending on what triggered the event
7.3.2.4 IIS / MSSQL / Exchange

These events are logged by IIS, Exchange Server and MSSQL server. Most Microsoft server applications (Backoffice) log extensive information to the event log and can thus be monitored very nicely with EventSentry.

<table>
<thead>
<tr>
<th>Event Log</th>
<th>ID</th>
<th>Type</th>
<th>Source</th>
<th>Category</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>221 9</td>
<td>Warning</td>
<td>MSExchange MTA</td>
<td>Field Engineering</td>
<td>The MTA is running recovery on the internal message database because the MTA was not shut down cleanly. This operation may take some time. Status updates will be written to the Windows 2000 Event Log.</td>
</tr>
<tr>
<td>Application</td>
<td>5</td>
<td>Error</td>
<td>MSExchange ES</td>
<td>General</td>
<td>An unexpected MAPI error occurred. Error returned was [0x800401548]</td>
</tr>
<tr>
<td>Application</td>
<td>120 02</td>
<td>Error</td>
<td>MSExchange IS</td>
<td>Content Engine</td>
<td>Error 8004011B-82000387 occurred while processing message &lt;&gt; from '<a href="mailto:somebody@aol.com">somebody@aol.com</a>'</td>
</tr>
<tr>
<td>Application</td>
<td>102 5</td>
<td>Warning</td>
<td>MSExchange IS Mailbox Store</td>
<td>General</td>
<td>An error occurred on database &quot;First Storage Group\Mailbox Store (SERVER1)&quot;. Function name or description of problem: Restrict/SetSearchCriteria Error: -1102 Warning: fail to apply search optimization to folder (FID 1-3619001) Retrying without optimization.</td>
</tr>
<tr>
<td>System</td>
<td>2</td>
<td>Information</td>
<td>IISCTLS</td>
<td>IIS stop command received from user DOMAIN\User. The logged data is the status code.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>Information</td>
<td>IISCTLS</td>
<td>IIS kill command received from user DOMAIN\User. The logged data is the status code.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>105</td>
<td>Error</td>
<td>W3SVC</td>
<td>The server was unable to register the administration tool discovery information. The administration tool may not be able to see this server. The data is the error code.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>100</td>
<td>Warning</td>
<td>W3SVC</td>
<td>The server was unable to logon the Windows NT account 'myaccount' due to the following error: Logon failure: unknown user name or bad password. The data is the error code.</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>105 1</td>
<td>Error</td>
<td>IMAP4SVC</td>
<td>General</td>
<td>Unexpected error condition: call to function CEncryptCtx::CheckServerCert() resulted in error code 0x800cc000.</td>
</tr>
<tr>
<td>System</td>
<td>50</td>
<td>Error</td>
<td>TermDD</td>
<td>The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>368 71</td>
<td>Error</td>
<td>Schannel</td>
<td>A fatal error occurred while creating an SSL server credential.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>368 72</td>
<td>Warning</td>
<td>Schannel</td>
<td>No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the directory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>368 74</td>
<td>Error</td>
<td>Schannel</td>
<td>An SSL connection request was received from a remote client application, but none of the cipher suites</td>
<td></td>
</tr>
</tbody>
</table>
The SSL connection request has failed.

**Applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>ID</th>
<th>Information</th>
<th>Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>17052</td>
<td>Information</td>
<td>MSSQL$Instance</td>
</tr>
<tr>
<td></td>
<td>17055</td>
<td>Information</td>
<td>MSSQL$Instance</td>
</tr>
<tr>
<td></td>
<td>17055</td>
<td>Information</td>
<td>MSSQL$Instance</td>
</tr>
<tr>
<td></td>
<td>20855</td>
<td>Information</td>
<td>SQLSERVERAGENT</td>
</tr>
</tbody>
</table>

**Error:** 154557, **Severity:** 0, **State:** 1

Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.

19013: SQL server listening on TCP, Shared Memory, Named Pipes.

19013: SQL Server listening on 34.234.34.32: 3431

17126: SQL Server is ready for client connections

Strings in italic may vary depending on what triggered the event.
# 7.3.2.5 Application Management

These events concern services and applications.

<table>
<thead>
<tr>
<th>Event Log</th>
<th>ID</th>
<th>Type</th>
<th>Source</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>26</td>
<td>Information</td>
<td>Application Popup</td>
<td>Application Popup: Service Control Manager : At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details.</td>
</tr>
<tr>
<td>System</td>
<td>26</td>
<td>Information</td>
<td>Application Popup</td>
<td>Application popup: somefile.exe - Application Error : The instruction at &quot;0x00000000&quot; referenced memory at &quot;0x00000000&quot;. The memory could not be &quot;read&quot;. Click on OK to terminate the program</td>
</tr>
<tr>
<td>System</td>
<td>7000</td>
<td>Error</td>
<td>Service Control Manager</td>
<td>The Simple Mail Transport Protocol (SMTP) service failed to start due to the following error: The system cannot find the file specified.</td>
</tr>
<tr>
<td>System</td>
<td>7031</td>
<td>Error</td>
<td>Service Control Manager</td>
<td>The Simple Mail Transport Protocol (SMTP) service terminated unexpectedly. It has done this 1 time(s). The following corrective action will be taken in 0 milliseconds: No action.</td>
</tr>
<tr>
<td>System</td>
<td>4381</td>
<td>Information</td>
<td>NTServicePack</td>
<td>Windows 2000 Service Pack 4 was installed.</td>
</tr>
<tr>
<td>System</td>
<td>4377</td>
<td>Information</td>
<td>NTServicePack</td>
<td>Windows 2000 Hotfix KB825119 was installed.</td>
</tr>
<tr>
<td>Security</td>
<td>592</td>
<td>Audit Success</td>
<td>Detailed Tracking</td>
<td>A new process has been created: New Process ID: 724 Image File Name: \Program Files\EventSentry\eventsentry_gui.exe Creator Process ID: 1044 User Name: Administrator Domain: GOAT Logon ID: (0x0,0xB6A9)</td>
</tr>
<tr>
<td>Security</td>
<td>593</td>
<td>Audit Success</td>
<td>Detailed Tracking</td>
<td>A process has exited: Process ID: 724 User Name: GOAT$ Domain: NETIKUS Logon ID: (0x0,0x3E7)</td>
</tr>
</tbody>
</table>

Strings in italic may vary depending on what triggered the event.
### 7.3.2.6 Hardware

These events are logged by hardware drivers, such as SCSI controllers, network card drivers etc. An event log entry is often the first indication that a hardware problem exists.

<table>
<thead>
<tr>
<th>Event Log</th>
<th>ID</th>
<th>Type</th>
<th>Source</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>4</td>
<td>Warning</td>
<td>b57w2k</td>
<td>Broadcom NetXtreme Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.</td>
</tr>
<tr>
<td>Application</td>
<td>1001</td>
<td>Warning</td>
<td>DPTELOG</td>
<td>The DISK at (0,0,0,0) returned SCSI status: Check Condition at Sun May 23 16:38:56 2004.</td>
</tr>
<tr>
<td>Application</td>
<td>1002</td>
<td>Error</td>
<td>DPTELOG</td>
<td>Non-corrected ECC RAM error found for device (0, 0, 0, 0) at Fri Jun 04 14:14:32 2004. RAM address: 0x809F2800</td>
</tr>
<tr>
<td>Application</td>
<td>1027</td>
<td>Warning</td>
<td>UPS Event</td>
<td>UPS disconnect! Cannot retrieve information from the UPS.</td>
</tr>
<tr>
<td>System</td>
<td>1</td>
<td>Error</td>
<td>afasa</td>
<td>\Device\Afa0: SMART WARNING: ID (0:2:0) =FPT_EXCEEDED</td>
</tr>
<tr>
<td>System</td>
<td>11</td>
<td>Error</td>
<td>Disk</td>
<td>The driver detected a controller error on \Device\Harddisk0\Partition2</td>
</tr>
</tbody>
</table>

*Strings in italic may vary depending on what triggered the event*
7.4 Examples & Templates

Please see the [How-To section on eventsentry.com](https://eventsentry.com) for a more comprehensive list of configuration examples and instructions.

7.4.1 Filter Examples

This section lists filter examples:

- **Example 1**: Standard Filter
- **Example 2**: Filter for event source
- **Example 3**: Filter for event source and multiple event IDs

7.4.1.1 Example 1: Standard Filter

This include filter monitors the Application and System event log for WARNING and ERROR messages and notifies an action named "Default Email" upon match.

Because all fields in the Details section are left blank any source, category, ID or username will match this filter.
7.4.1.2 Example 2: Event Source

This include filter monitors the Security event log for **AUDIT SUCCESS** and **AUDIT FAILURE** messages and notifies a target named "Default Email" upon match.

Additionally, only events from the source "Security Account Manager" will match this filter.
7.4.1.3 Example 3: Event Source & Event ID

This include filter monitors the Application event log for INFORMATION, WARNING and ERROR messages and notifies an action named “Default Email” upon match.

Additionally only events from the source “Diskeeper” with Event IDs 15,16,17,18 and 19 will match this filter.
7.4.1.4 Example 4: Content Filter with Insertion String

The purpose of this filter will be to trigger an action when the temperature reported by the EventSentry temperature sensor exceeds 80 degrees F. A typical event would look like this:
Looking at the 10908 event with the event message browser reveals the following:

The temperature (%3 degrees %4) has fallen outside the configured range (%1% to %2%).

Since insertion string #3 is being substituted with the temperature, we will create a content filter which looks at the third insertion string.

Since the insertion string #3 is a number, we can take advantage of the numerical comparison, as shown above. The main filter dialog will then look similar to this:
7.4.2 Summary Notification Examples

This section lists Summary Notification Examples:

Example 1: Daily Summary

Example 2: Daily Summary with Messages

7.4.2.1 Example 1: Daily Summary

This notification filter notifies the specified action (not shown) every day at 9 am and 7 pm. Please note that notifications are always sent out at the end of the active hour, 9 am and 7 pm in this particular case.
7.4.2.2 Example 2: Daily Summary with Messages

This example notification filter notifies the specified action (not shown) every day at 7 pm. Events between 7 pm and 8 am are forwarded in real-time, unless controlled by another filter.
7.5 Compliance

7.5.1 Matrix

The matrix below shows which compliance sections are covered by EventSentry (tracking) features.

**Report Title**
- Feature: Path to the query page in the EventSentry web reports
- Report: Name of the built-in report, if available and applicable. Reports are accessed through EVENT -> REPORTS

### Active Directory Administrator Logons

<table>
<thead>
<tr>
<th>Feature</th>
<th>PCI</th>
<th>FISMA / NIST 800 53</th>
<th>ISO17799</th>
<th>Cobit</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Compliance -&gt; Logon Tracking -&gt; Console Logons</td>
<td>AC-13 AO-2 AO-3 AU-6 AU-7</td>
<td>0.5 10.1.3 10.10. 10.10. 10.10. 10.10. 11.5.1 11.5.115.1 115.1 115.1 15.1 15.2.15.3.</td>
<td>PO 4.11 PO 7.8 AI 2.3 AI 2.4 AI 4.2 AI 6.4 AI 6.5 DS 5.5 DS 5.4</td>
<td>164.306 164.30164.31164.31164.31</td>
</tr>
<tr>
<td>Report:</td>
<td>Administrative Console Logons</td>
<td></td>
<td></td>
<td></td>
<td>8a 2a 2b 2d</td>
</tr>
</tbody>
</table>

### Active Directory General Object Changes

<table>
<thead>
<tr>
<th>Feature</th>
<th>PCI</th>
<th>FISMA / NIST 800 53</th>
<th>ISO17799</th>
<th>Cobit</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Event -&gt; Event Search</td>
<td>AC-13 AO-2 AO-3 AU-6</td>
<td>0.5 10.1.3 10.10. 10.10. 10.10. 10.10. 11.5.1 11.5.115.1 115.1 115.1 15.1 15.2.15.3.</td>
<td>PO 4.11 PO 7.8 AI 2.3 AI 2.4 AI 4.2 AI 6.4 AI 6.5 DS 5.5 DS 5.4</td>
<td>164.306 164.30164.31164.31164.31</td>
</tr>
<tr>
<td>Report:</td>
<td>Active Directory General Object Changes</td>
<td></td>
<td></td>
<td></td>
<td>8a 2a 2b</td>
</tr>
</tbody>
</table>

### Active Directory Group Member Additions

<table>
<thead>
<tr>
<th>Feature</th>
<th>PCI</th>
<th>FISMA / NIST 800 53</th>
<th>ISO17799</th>
<th>Cobit</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Compliance -&gt; Account Changes -&gt; Group Account</td>
<td>AC-2 AC-13 AO-2 AO-3 AU-6</td>
<td>0.5 10.1.3 10.10. 10.10. 10.10. 10.10. 11.5.1 11.5.115.1 115.1 115.1 15.1 15.2.15.3.</td>
<td>PO 4.11 PO 7.8 AI 2.3 AI 2.4 AI 4.2 AI 6.4 AI 6.5 DS 5.5 DS 5.4</td>
<td>164.306 164.30164.31164.31164.31</td>
</tr>
<tr>
<td>Report:</td>
<td>Active Directory Security Group Changes</td>
<td></td>
<td></td>
<td></td>
<td>8a 2a 2b</td>
</tr>
</tbody>
</table>
Active Directory Group Member Deletions
Feature: Compliance -> Account Changes -> Group Account
Report: Active Directory Security Group Changes

Active Directory New or Enabled Account
Feature: Compliance -> Account Changes -> User Account
Report: Active Directory User Changes

Active Directory Users Deleted or Disabled
Feature: Compliance -> Account Changes -> User Account
Report: Active Directory User Changes

Active Directory Group Policy Change Report
Feature: Event -> Event Search
Report: Active Directory Group Policy Changes

PCI 6.4 7.1 10.1 10.2 10.3 10.5 10.6 10.7
FISMA / NIST AC-2 AC-13 PS-6 AU-2 AU-3 AU-6 AU-7 AU-9
ISO17799 0.5 8.3.3 10.1.2 10.10. 10.10. 10.10.11.12.5.13.2.13.2.15.1.15.2.15.3.
1 2 3 4 1 1 3 3 1 1
Cobit PO 4.11 PO 7.8 Al 2.3 Al 2.4 Al 4.2 Al 6.4 Al 6.5 DS DS ME ME ME ME
5.4 5.5 2.3 2.5 3.4 4.4 4.5 4.7
HIPAA 164.306 164.30164.31164.31
8a 2a 2b 2d

PCI 6.4 7.1 10.1 10.2 10.3 10.5 10.6 10.7
FISMA / NIST AC-2 AU-2 AU-3 AU-6 AU-7 AU-9
ISO17799 0.5 8.3.3 10.1.2 10.10. 10.10. 10.10.11.12.5.13.2.13.2.15.1.15.2.15.3.
1 2 3 4 1 1 3 3 1 1
Cobit PO 4.11 PO 7.8 Al 2.4 AI 4.2 Al 6.4 DS 5.3 DS DS ME
5.4 5.5 2.5
HIPAA 164.306 164.30164.31164.31164.31
8a 2a 2b 2d 2e
### Active Directory Permission Changes

**Feature:** Event -> Event Search  
**Report:** Active Directory General Object Changes  

<table>
<thead>
<tr>
<th>PCI</th>
<th>6.4</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AC-3</td>
<td>AC-13</td>
<td>AU-2</td>
<td>AU-3</td>
<td>AU-6</td>
<td>AU-7</td>
<td>AU-9</td>
</tr>
<tr>
<td>ISO17799</td>
<td>0.5</td>
<td>10.1.2</td>
<td>10.1.3</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.11.1.12.5.13.2.13.2.15.1.15.2.15.3.</td>
</tr>
<tr>
<td>Cobit</td>
<td>PO 4.11</td>
<td>AI 2.3</td>
<td>AI 2.4</td>
<td>AI 4.2</td>
<td>AI 6.4</td>
<td>AI 6.5</td>
<td>DS ME ME ME ME</td>
</tr>
<tr>
<td>HIPAA</td>
<td>164.306 164.30164.31164.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8a</td>
<td>2a</td>
<td>2b</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Active Directory User Account Lockouts and Password Resets

**Feature:** Compliance -> Account Changes -> User Account  
**Report:** Active Directory User Changes  

<table>
<thead>
<tr>
<th>PCI</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AC-2</td>
<td>AC-7</td>
<td>AU-2</td>
<td>AU-3</td>
<td>AU-6</td>
</tr>
<tr>
<td>ISO17799</td>
<td>0.5</td>
<td>10.1.3</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
</tr>
<tr>
<td>Cobit</td>
<td>PO 4.11</td>
<td>AI 3.2</td>
<td>AI 4.2</td>
<td>DS 5.4</td>
<td>DS</td>
</tr>
<tr>
<td>HIPAA</td>
<td>164.306 164.30164.31164.31164.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8a</td>
<td>2a</td>
<td>2b</td>
<td>2d</td>
<td></td>
</tr>
</tbody>
</table>

### Active Directory Domain Policy Changes

**Feature:** Compliance -> Policy Changes -> Domain Policy  
**Report:** Active Directory Domain Policy Changes  

<table>
<thead>
<tr>
<th>PCI</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AC-3</td>
<td>AC-13</td>
<td>AU-2</td>
<td>AU-3</td>
<td>AU-6</td>
<td>AU-7</td>
</tr>
<tr>
<td>ISO17799</td>
<td>0.5</td>
<td>10.1.2</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
<td>12.5.1</td>
</tr>
<tr>
<td>Cobit</td>
<td>PO 4.11</td>
<td>AI 2.3</td>
<td>AI 2.4</td>
<td>AI 4.2</td>
<td>AI 6.4</td>
<td>AI 6.5</td>
</tr>
<tr>
<td>HIPAA</td>
<td>164.306 164.30164.31164.31164.31164.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8a</td>
<td>2a</td>
<td>2b</td>
<td>2c</td>
<td>2d</td>
<td>2e</td>
</tr>
</tbody>
</table>
### Local Group Member Additions Report

**Feature:** Compliance -> Account Changes -> Group Account  
**Report:** Member Server Security Group Changes

<table>
<thead>
<tr>
<th>PCI</th>
<th>6.4</th>
<th>7.1</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AC-2</td>
<td>AC-13</td>
<td>AU-2</td>
<td>AU-3</td>
<td>AU-6</td>
<td>AU-7</td>
<td>AU-9</td>
<td></td>
</tr>
<tr>
<td>800 53</td>
<td>ISO17799</td>
<td>0.5</td>
<td>10.1.2</td>
<td>10.1.3</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
<td>12.5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Cobit</td>
<td></td>
<td></td>
<td>PO 4.11</td>
<td>PO 7.8</td>
<td>Al 2.3</td>
<td>Al 2.4</td>
<td>Al 4.2</td>
<td>Al 6.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.5</td>
<td>2.3</td>
<td>2.5</td>
<td>3.4</td>
<td>4.4</td>
<td>4.5</td>
</tr>
<tr>
<td>HIPAA</td>
<td>164.306</td>
<td>164.30164.31164.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8a</td>
<td>2a</td>
<td>2b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Local Group Member Deletions Report

**Feature:** Compliance -> Account Changes -> Group Account  
**Report:** Member Server User Changes

<table>
<thead>
<tr>
<th>PCI</th>
<th>6.4</th>
<th>7.1</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AC-2</td>
<td>AC-13</td>
<td>AU-2</td>
<td>AU-3</td>
<td>AU-6</td>
<td>AU-7</td>
<td>AU-9</td>
<td></td>
</tr>
<tr>
<td>800 53</td>
<td>ISO17799</td>
<td>0.5</td>
<td>8.3.3</td>
<td>10.1.2</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cobit</td>
<td></td>
<td></td>
<td>PO 4.11</td>
<td>PO 7.8</td>
<td>Al 2.3</td>
<td>Al 2.4</td>
<td>Al 4.2</td>
<td>Al 6.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.4</td>
<td>5.5</td>
<td>2.3</td>
<td>2.5</td>
<td>3.4</td>
<td>4.4</td>
</tr>
<tr>
<td>HIPAA</td>
<td>164.306</td>
<td>164.30164.31164.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8a</td>
<td>2a</td>
<td>2b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Local Users Consolidated Changes

**Feature:** Compliance -> Account Changes -> User Account  
**Report:** Member Server User Changes

<table>
<thead>
<tr>
<th>PCI</th>
<th>6.4</th>
<th>7.1</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AC-2</td>
<td>AC-13</td>
<td>PS-6</td>
<td>AU-2</td>
<td>AU-3</td>
<td>AU-6</td>
<td>AU-7</td>
<td>AU-9</td>
</tr>
<tr>
<td>800 53</td>
<td>ISO17799</td>
<td>0.5</td>
<td>10.1.2</td>
<td>10.1.3</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
<td>12.5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Cobit</td>
<td></td>
<td></td>
<td>PO 4.11</td>
<td>PO 7.8</td>
<td>Al 2.3</td>
<td>Al 2.4</td>
<td>Al 4.2</td>
<td>Al 3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.4</td>
<td>5.5</td>
<td>2.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>164.306</td>
<td>164.30164.31164.31164.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8a</td>
<td>2a</td>
<td>2b</td>
<td>2d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Object Access

**Feature:** Compliance -> File Access  
**Report:** n/a

<table>
<thead>
<tr>
<th>PCI</th>
<th>6.4</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AU-3</td>
<td>AU-6</td>
<td>AU-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>800 53</td>
<td>ISO17799</td>
<td>0.5</td>
<td>10.6.1</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
<td>10.10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>
### Object Deletions

**Feature:** Compliance -> File Access  
**Report:** n/a

| **PCI** | 6.4 | 10.1 | 10.2 | 10.3 | 10.5 | 10.6 | 10.7 |
| **FISMA / NIST 800 53** | AC-13 | AU-2 |
| **ISO17799** | 0.5 | 10.6 | 10.10 | 10.10 | 13.2 | 13.3 | 15.6 | 15.3 | 15.2 | 15.1 |
| **Cobit** | AI 2.3 | DS | DS 9.2 | ME 2.3 | ME 2.5 | ME 3.4 | 4.4 |
| **HIPAA** | 164.306 | 164.301 | 164.31 | 164.31 | 8a | 2a | 2b |

### Permission Changes

**Feature:** Compliance -> File Access  
**Report:** n/a

| **PCI** | 6.4 | 7.1 | 10.1 | 10.2 | 10.3 | 10.5 | 10.6 | 10.7 |
| **FISMA / NIST 800 53** | AC-13 | AU-2 |
| **ISO17799** | 0.5 | 10.6 | 10.10 | 10.10 | 10.10 | 10.10 | 11.1 | 11.6 | 1 |
| **Cobit** | AI 2.3 | AI 2.4 | DS | ME 2.3 | ME 2.5 | ME 3.4 | 4.4 |
| **HIPAA** | 164.306 | 164.301 | 164.31 | 164.31 | 8a | 2a | 2b |

### Programs Executed By User

**Feature:** Compliance -> Process Tracking  
**Report:** n/a

| **PCI** | 10.1 | 10.6 |
| **FISMA / NIST 800 53** | MA-3 | AC-13 | AU-2 |
| **ISO17799** | 0.5 | 10.10 | 10.10 | 10.10 | 10.10 | 11.5 | 4 | 15.1 | 2 |
| **Cobit** | PO 4.11 | AI 1.3 | AI 2.3 | AI 2.4 | DS | ME 2.5 | ME 3.4 | ME 4.4 |
| **HIPAA** | 164.306 | 164.301 | 164.31 | 164.31 | 8a | 2a | 2b |

### Programs Executed Summary

**Feature:** Compliance -> Process Tracking
User Activity
Journal
Feature: Compliance -> Process Tracking
Report: n/a

Major Security Events and Policy Changes
Feature: Compliance -> Policy Changes
Report: Active Directory Domain Policy Changes
Active Directory Audit Policy Changes
Active Directory Kerberos Policy Changes
Active Directory Trust Relationship Changes

Domain Account Authentication
Feature: Compliance -> Logons -> Network
Report: Domain Account Authentication
Domain Account Authentication Failure Analysis

Feature: Compliance -> Logons -> Failures
Report: Domain Account Authentication Failure Analysis

PCI
10.2 10.3 10.5 10.6 10.7

FISMA / NIST
AC-13 AU-2 AU-3 AU-6 AU-7 AU-9

ISO17799
0.5 10.1.3 10.10. 10.10. 10.10. 10.10. 11.5.2 11.5.3 13.2.15.1.15.2.15.3.
1 2 3 3 3 3 1 1

Cobit
PO 4.11 DS ME 2.1 ME 2.5 5.5

HIPAA
164.306 164.30164.31164.31164.31
8a 2a 2b 2d

Initial Logon With Servers Accessed

Feature: Compliance -> Logons -> Network
Report: n/a

PCI
10.2 10.3 10.5 10.6 10.7

FISMA / NIST
AC-2 AU-2 AU-3 AU-6 AU-7 AU-9

ISO17799
10.10.1 10.10. 10.10. 15.1.5
2 3

Cobit

HIPAA

Member Server Authentication

Feature: Compliance -> Logons -> Network
Report: n/a

PCI
10.2 10.3 10.5 10.7

FISMA / NIST
AC-13 AU-2 AU-3 AU-6 AU-7 AU-9

ISO17799
0.5 10.1.3 10.10. 10.10. 10.10. 10.10. 11.5.2 11.5.3 13.2.15.1.15.2.15.3.
1 2 3 3 3 3 1 1

Cobit
PO 4.11 DS ME 2.1 ME 2.5 5.5

HIPAA

User Authentication And Logon Journal

Feature: Compliance -> Logons -> Network
Report: n/a
### User Logons By Server-Type

**Feature:** Compliance -> Logons -> By Type  
**Report:** Logons: By Server-Type

<table>
<thead>
<tr>
<th>PCI</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISMA / NIST</td>
<td>AC-2</td>
<td>AU-2</td>
<td>AU-3</td>
<td>AU-6</td>
<td>AU-7</td>
<td>AU-9</td>
</tr>
<tr>
<td>ISO17799</td>
<td>10.1.1</td>
<td>10.10.10.10.15.1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CoBit</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>164.306</td>
<td>164.30164.31164.31164.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8a</td>
<td>2a</td>
<td>2b</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 7.5.2 Regulations

Depending on which type of regulatory compliance an organization has to comply with, the following topics can be used as a starting point to determine which reports in EventSentry need to be evaluated and generated on a regular basis.

Once the appropriate reports have been selected, optionally customized and a schedule determined, then the Review feature of the reports can be used to ensure that reports are actually being run at the required time intervals.

A blue cell in the table indicates that the report helps fulfill this particular section. For example, the *Active Directory Users Deleted or Disabled*, *Active Directory - User Account Lockouts and Password Resets* and *Active Directory Domain Policy Changes* are relevant for section 164.312e of HIPAA.

#### 7.5.2.1 PCI

<table>
<thead>
<tr>
<th>Active Directory Administrator Logons</th>
<th>6.1</th>
<th>7.1</th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.4</th>
<th>10.5</th>
<th>10.6</th>
<th>10.7</th>
<th>10.8</th>
<th>10.9</th>
<th>10.10</th>
<th>10.11</th>
<th>10.12</th>
<th>10.13</th>
<th>10.14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory General Object Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Additions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Deletions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory New or Enabled Account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Users Deleted or Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Policy Change Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Permission Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - User Account Lockouts and Password Resets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - Users Groups and Computers Consolidated Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Active Directory Domain Policy Changes
Local Group Member Additions Report
Local Group Member Deletions Report
Local Users Consolidated Changes
Object Access
Object Deletions
Permission Changes
Programs Executed By User
Programs Executed Summary
User Activity Journal
Major Security Events and Policy Changes
Domain Account Authentication
Domain Account Authentication Failure Analysis
Initial Logon With Servers Accessed
Member Server Authentication
User Authentication And Logon Journal
User Logons By Server - Type

### 7.5.2.2 FISMA NIST 800-53

<table>
<thead>
<tr>
<th></th>
<th>MA-3</th>
<th>AC-2</th>
<th>AC-3</th>
<th>AC-7</th>
<th>AC-13</th>
<th>PS-6</th>
<th>AU-2</th>
<th>AU-3</th>
<th>AU-6</th>
<th>AU-7</th>
<th>AU-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Administrator Logons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory General Object Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Additions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Deletions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory New or Enabled Account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Users Deleted or Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Policy Change Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Permission Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - User Account Lockouts and Password Resets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - Users Groups and Computers Consolidated Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Domain Policy Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Group Member Additions Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Group Member Removal Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Users Consolidated Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Deletions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programs Executed By User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programs Executed Summary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Activity Journal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major Security Events and Policy Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Account Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Account Authentication Failure Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial Logon With Servers Accessed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member Server Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## User Authentication And Logon Journal

### User Logons By Server - Type

### 7.5.2.3 ISO 17799

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Administrator Logons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory General Object Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Additions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Deletions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory New or Enabled Account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Users Deleted or Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Policy Change Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Permission Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - User Account Lockouts and Password Resets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - Users Groups and Computers Consolidated Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Domain Policy Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Group Member Additions Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Group Member Deletions Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Users Consolidated Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major Security Events and Policy Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Deleted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programs Executed By User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programs Executed Summary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Activity Journal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Account Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Account Authentication Failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Analysis

- Initial Logon With Servers Accessed
- Member Server Local Account Authentication
- User Authentication And Logon Journal
- User Logons By Server - Type

#### 7.5.2.4 CobiT / Sarbanes Oxley

<table>
<thead>
<tr>
<th>Event Type</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Administrator Logons</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory General Object Changes</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory Group Member Additions</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory Group Member Deletions</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory Users - New or Enabled</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory Users Deleted or Disabled</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory Group Policy Change Report</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory Permission Changes</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory - User Account Lockouts and Password Resets</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory - Users Groups and Computers Consolidated Changes</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Active Directory Domain Policy Changes</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Local Group Member Additions Report</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Local Group Member Deletions Report</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Local Users Consolidated Changes</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Major Security Events and Policy Changes</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Object Access Report</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Object Deleted</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Permission Changes</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Programs Executed By User Report</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Programs Executed Summary</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Domain Account Authentication Failure Analysis</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Domain Account Authentication</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>User Logons By Server - Type</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>User Activity Journal</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Member Server Local Account Authentication</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
<td>O</td>
<td>P</td>
</tr>
</tbody>
</table>
7.5.2.5  HIPAA

<table>
<thead>
<tr>
<th>Feature</th>
<th>164.30 6</th>
<th>164.30 8a</th>
<th>164.31 2a</th>
<th>164.31 2b</th>
<th>164.31 2c</th>
<th>164.31 2d</th>
<th>164.31 2e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Administrator Logons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory General Object Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Additions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Member Deletions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory New or Enabled Account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Users Deleted or Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Group Policy Change Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Permission Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - User Account Lockouts and Password Resets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory - Users Groups and Computers Consolidated Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Domain Policy Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Group Member Additions Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Group Member Removal Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Users Consolidated Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major Security Events and Policy Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Access Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Deleted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permission Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programs Executed Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programs Executed Summary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Account Authentication Failure Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Account Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Logons By Server - Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Activity Journal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.6  Miscellaneous

7.6.1  File Monitoring vs. File Access Tracking

The File Monitoring (System Health) and File Access Tracking (Security & Compliance) features can seem ambiguous since they both monitor file changes. The features are quite different however and attempt to solve different problems. The comparison table below outlines the key differences between these features:

**Comparison Overview**

<table>
<thead>
<tr>
<th>Feature</th>
<th>File Monitoring</th>
<th>File Access Tracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can generate alerts, trigger actions</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Requires NTFS auditing to be enabled on monitored folder(s)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Captures username who accessed and/or modified file</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can capture calling process who accessed and/or modified file</td>
<td>No</td>
<td>Yes, depending on source</td>
</tr>
<tr>
<td>Can capture source computer from which file was accessed and/or modified</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
System Health -> File Monitoring

This feature monitors files in one or more designated directories either in real-time or in scheduled intervals. File Monitoring was designed with both security (integrity checks) and system automation in mind, and is primarily intended to issue alerts or trigger actions when a file change is detected.

From a security standpoint, File Monitoring ensures that selected files (e.g. executables in the SYSTEM32 directory, credit card transaction logs and so forth) are not changed, and that any change that does occur is logged and, optionally, triggers an alert.

From a system administrator standpoint, it can help automate many tasks that are triggered based on file changes in a directory. For example, a directory can be monitored and any file added to the directory can be automatically compressed by a process action, or a list of users can be notified that a file has been added. Since file changes can be directly linked to a process action, the abilities of what one can do are only limited by the process/batch file itself.

One distinct advantage of the File Monitoring feature is that it does not require any additional configuration steps on the OS. Once File Monitoring is configured and the configuration pushed, it will be effective immediately.

Security & Compliance -> File Access Tracking

Security & Compliance intercepts "Object Access" security events which are generated by the Operating System when auditing has been enabled on a file and/or directory. This feature was designed to monitor directories that contain confidential or security-sensitive data, and provide advanced reporting that can be used to satisfy both security and compliance-related demands.

While File Access Tracking cannot generate any type of alert or trigger actions, it does include more information about the file changes themselves. The key advantage is that File Access Tracking can often let you know who made changes to a file, and from where.

For example, depending on the source of the file change, the tracking information may include the calling process as well as the source computer.

Due to some key architectural differences between Pre-Vista operating systems, Vista and Windows Server 2008 are the preferred platforms for this feature, though earlier operating systems are fully supported as well.

Keep in mind that File Access Tracking requires that NTFS auditing is enabled on any folder that needs to be monitored, see File Access Tracking Prerequisites for more information.
8  Support, FAQ, Version History

8.1  Troubleshooting and FAQ

Please search our knowledge base at https://www.eventsontry.com/support/kb for answers to known problems. Our knowledge base is under constant development and contains answers to the most commonly asked questions and problems about EventSentry.

---

Knowledge Base

I cannot install or update EventSentry on some or all remote computers using Remote Update. Some of the error messages reported are: Access Denied, Remote Procedure Call (RPC) failed. EventSentry uses Windows RPC calls to update remote agents and remote update forwards all error messages reported by Windows when a remote update fails. EventSentry uses the following features: Remote Service Control connecting to the remote SCM service control manager. File access EventSentry installs all required agent files to ...

KB-ID 51  Category: Usage  Applies to: All Versions

When upgrading the EventSentry agent on a remote host that is running a 64-bit edition of Windows using remote update, the remote agent (service) fails to start. You may also get the error "Unable to update service configuration, please see KB 164 at eventsentry.com"

Starting with version 2.90 the EventSentry agent eventsontry.exe is installed in the SYSTEMROOT\SysWOW64 directory on 64-bit machines. When updating from EventSentry 2.81 or earlier to EventSentry 2.90 or later the service configuration needs to be updated in order for the service configuration to point to the new location of the...

KB-ID 164  Category: Installation  Applies to: 2.90

The EventSentry agent is not installed or stopped.

EventSentry requires the EventSentry agent to be installed and running on all machines that you need to monitor. If the agent is not installed or stopped no monitoring will occur. If the EventSentry is stopped then you can either start it by opening up the Services control panel selecting the EventSentry service and starting it or you can...

---

8.2  Questions or Problems?

Please note that we can only guarantee to answer support requests that are sent from registered email addresses (by default the one you specified when EventSentry was purchased).

EventSentry Light Users

If you are using the free version of EventSentry, EventSentry Light, then you can obtain support through the NETIKUS.NET Support Forums at https://helpdesk.eventsentry.com/, or by browsing the knowledge base at http://www.eventsentry.com/support/kb.

Questions

If you still have questions after reading this manual then please

- send an email to support@netikus.net or
- call 1-877-NETIKUS (1-877-638-4587)

and include the following information:

- The Operating System (incl. Service Pack Version) on which EventSentry is running
problems
If you are experiencing problems with EventSentry then you can either fill out the Bug / Problem Report feedback form in the Feedback menu or

- send an email to support@netikus.net
- call 1-877-NETIKUS (1-877-638-4587)

and include the following information:

- The Operating System (incl. Service Pack Version) on which EventSentry is running
- The version of EventSentry
- An exact description of the problem. Include information such as:
  - Does this problem occur on one or more installations?
  - Did it happen once or does it happen repeatedly?
  - What can we do to reproduce the problem?

8.3 Version History
This page lists all versions of EventSentry that were released since its initial launch in December 2002 until 2017. A complete version history of all versions is available online.

To learn more about the numbering system click here.

Version 3.4.1  September 2017

Windows Monitoring
- Additional capabilities to detect and prevent against new types of Ransomware infections, including variants that modify the boot sector.
- New software version check identifies outdated software on your network to help you reduce your attack surface. This new feature supplements EventSentry’s software inventory component.
- Disk space alerts now include a list of the largest files and folders of a volume
- UPS & Battery monitoring now inventories all attached UPS batteries as well as integrated batteries (laptops) regardless of the manufacturer
- Effective audit settings on a Windows host can sometimes deviate from group policy settings - due to conflicts, errors and so forth. A new Audit Policy Status page periodically inventories the current audit settings so you can verify the actual audit settings.

Network Monitoring
- NetFlow monitoring now supports calculating the bandwidth of an interface, including additional statistics such as packet count, bytes per packet and more.
- Ping response time now provides packet loss stats

Integrations
- EventSentry agents can now be integrated with many open source and commercial log solutions with additional Syslog options - even custom JSON formatting is supported!

Web Reports
- Now available in 64-bit and support larger reports and increased performance
New user activity tracking page makes seeing all activity by a user as easy as never before!

Version 3.3.1  December 2016

NetFlow
- NetFlow with support for NetFlow v1, v5, v9 & sFlow. NetFlow supports visualization, geolocation, alerts, correlation with workstation logon events to map flows to ActiveDirectory users, filtering and more

Web Reports
- Notes & Documentation: Web reports users can submit notes to document infrastructure updates, maintenance, fixes and more. Documentation files can be uploaded and associated with hosts
- Added ISO 27001:2013 compliance reports
- New security features
- New dashboard tiles
- Treemap visualization available for most pages
- Updated look and improved menu

Management Console
- Deployment: Agents using the collector can receive configuration and agent binary updates automatically through the collector without user intervention.
- Deployment: MSI installers can now be created in a few seconds directly from the management console (requires free WiX Toolset)
- Ability to reset the configuration to post-installation defaults (new v3.3 installations only)
- Remote configuration can now removed when uninstalling an agent even when remote registry service is unavailable
- Version checks and update/patch downloads are now performed over TLS for enhanced security

Agent
- 64-bit agent is now available for 64-bit Windows
- Removed limit and improved management of custom event logs
- Support for chaining events
- Agent / Collector: Emails containing IP addresses sent through collector can be enhanced to display geolocation and reverse lookup data inline.
- Emails from security event log will automatically be enhanced with descriptions for many status and error codes
- Database performance of delimited log files has been significantly improved
- Insertion strings of events can be created or replaced using regular expressions
- Install date of software is now available for most software even if it was installed before EventSentry
- USB drives are now detected in real-time

Other
- Heartbeat Agent: Agent status is now retrieved directly from collector and/or database for faster and more efficient monitoring
- Network Services: Database performance for Syslog component has been improved for MSSQL databases
- Network Services: License count for network devices is now more accurately enforced
- Database: Built-In database now uses PostgreSQL v9.6, optional upgrade path is available
Configuration: Improved out-of-the-box filter rules for less noise

Version 3.2.1  February 2016

Collector
- Central collector service which enables a 3-tier architecture between an action (e.g. database, email server) and the EventSentry agents
- Supports compression and secure data transmission via TLS encryption

General
- Management Console: Ability to import computers from a network (subnet) scan
- Management Console / Remote Update: Record activity in log files
- Management Console / Remote Update: Toggle fields in result list
- Management Console: Export all configured filters to CSV file
- Switch inventory with switch port to MAC/hostname mapping
- Detection of highest supported USB version

Web Reports
- Additional language support for French, Spanish, Polish, Portuguese and Italian
- Out-of-the-box compliance reports for PCI-DSS, FISMA, Sarbanes Oxley, HIPAA and GLBA
- Improved & faster performance trend reporting with ability to display multiple trend charts on a single page
- New Bulk assignment for easier report management
- Report jobs can be saved to a folder
- Improved host inventory page now shows switch port (if available), USB version and VM hosts (if available)
- Health matrix displays computer notes
- Improved usability throughout
- Improved connection pool support

Version 3.1.1  December 2014

Windows & General Monitoring
- Task Scheduler inventory and change detection
- Large File enumeration
- Inventory of virtual machines (Hyper-V & ESXi)
- HTTP action now supports POST/PUT for better interoperability with web-based APIs
- Disk space monitoring now supports multiple disk space packages assigned to a single host
- Improved remote update / host management, especially of Non-Windows hosts in management console

Heartbeat & SNMP Monitoring
- Process Monitoring support for SNMP-enabled hosts
- Improved router functionality, configure routers based on IP subnet
- Status change detection and uptime calculation is more reliable
- Overall stability improvements in the heartbeat agent

Web Reports
- Support for multiple dashboards, including automatic iteration between dashboards
- Dashboards can be shared
- Support for graphical gauges (Clock, meter, number, bullet)
- New heat-map tile for uniquely visualizing log, syslog and performance data
• New generic search tile supports embedding data from any feature in dashboard
• Support for TV mode and dark/light theme in dashboard
• Various tweaks and improvements to existing dashboard tiles

Version 3.0.1  December 2013

New Web Reports
• Scheduled Jobs: Receive reports via email
• PDF & JSON Output
• UTC Support
• Cross-platform: Supports Windows, Linux and OS X
• Complex queries for all features
• Full API
• Easier installation & setup
• Better dashboards
• Better summary pages
• Do no longer require Flash
• Access control with LDAP integration

Network Monitoring (Heartbeat Agent)
• Poll SNMP counters (integrates with performance monitoring)
• Retrieve disk space information from SNMP-enabled hosts
• Retrieve basic system & hardware information from SNMP-enabled hosts
• Retrieve uptime from SNMP-enabled hosts

Windows Monitoring
• Log file monitoring supports sub folders
• Compliance "Logon By Type" tracking can exclude logons by computer accounts
• Event Log filters can override email subject & message body
• Packages can by dynamically assigned based on platform (32bit vs 64bit)
• Threshold filters can utilize insertion strings
• Disk space prediction feature (predicts when disk will be full)
• Identify reasons why hosts were shut down or rebooted
• Desktop notification supports Growl
• Network notification supports remote desktop services
• Application scheduler support process isolation
• New email format "HTML Modern"

Other
• New management console features ribbon & visual improvements
• New authentication manager
• Many common tasks have been simplified
• Improved built-in event viewer for Application & Services Logs
• ARP daemon detects & tracks new MAC addresses and MAC to IP mappings

Version 2.93  June 2012

New Features:
• New installer for a better installation and upgrade experience
• Now includes a built-in (PostgreSQL) database
• Added support for PostgreSQL 9.x
• ODBC drivers for PostgreSQL and MySQL are now installed automatically (when needed)
• New installation includes performance monitoring packages for Exchange Server and others
• Preliminary support for Windows 8 and Windows Server 2012
• Support for USB-only temperature & humidity sensors
• Introducing the Configuration Assistant, which supersedes the database setup wizard, and introduces additional functionality
• Heartbeat monitoring can now scan hosts in parallel using multiple threads
• Heartbeat monitoring: Maintenance schedule can be set to the “nth” weekday (e.g. 2nd Tuesday)
• Performance Monitoring supports floating point counter values
• Performance Monitoring can log counter data to multiple databases
• Performance Monitoring can combine values from two different counters
• Performance Monitoring can detect leaks in performance counters
• Performance Monitoring can suppress alerts based on past values
• Performance Monitoring alerts are more verbose and include additional information, including counter descriptions
• Process Monitoring: Supports wildcards and can evaluate the command line of a process
• Event Log Backups: Better alerts and alerts now include SHA checksum of .evt(x) files
• Event Log Monitoring: Content filter supports perl regular expression syntax
• Event Log Monitoring: Day/Hour filter can be set to the “nth” weekday (e.g. 2nd Tuesday)
• Event Log Monitoring: For Windows 2008 and later, processing performance has been optimized for higher throughput and lower CPU usage
• Process Monitoring: Now collects process elevation level when UAC is enabled
• Embedded scripts now verify temp file contents with checksum
• Embedded scripts called from the applications scheduler now support command-line arguments
• Hardware Inventory: On DELL & HP servers (when required manufacturer management tools are installed), collects fan speed, redundant power supply status, remote management card information, temperature information, detailed RAID information
• Hardware Inventory: Retrieves warranty information for DELL, HP, IBM and Lenovo hardware
• Hardware Inventory: Retrieves configured UAC level
• Actions: Filter notes can now be posted to HTTP action
• Management Console: Saving configuration is about 10 times faster
• Management Console: Added better keyboard and mouse scroll wheel navigation for better user experience and section 508 compliance
• Management Console: Status of all local EventSentry services is now monitored in the background
• Management Console: Environment monitoring dialog now shows serial ports with descriptions
• Web Reports: Performance Status and Heartbeat Status pages load significantly faster
• IIS: IIS no longer has to be switched to 32-bit mode on 64-bit systems

**Bug Fixes:**

• Added support for 64-bit event numbers (Vista and later)
• Audit policies for compliance tracking features are now set correctly on Vista and later systems
• Resolved problems in various features when Japanese file names were processed
• Computer names exceeding the maximum NetBIOS length of 15 characters are now properly stored in the database
• Event message text is now properly formatted before submitting to SNPP (Pager) server
• Software Inventory: Internet Explorer is now properly detected on Vista and later
- Software Inventory: Patches are new enumerated even when TrustedInstaller.exe is active
- Event Log Backup: Resolved small memory leak
- Heartbeat Monitoring: Improved reliability
- Heartbeat Monitoring: Resolved memory leaks
- Environment Monitoring: Location is now included in alerts
- Performance Monitoring: Performance Status and other related pages (including network status, mobile apps) now load significantly faster
- Fixed bugs in Console Logon Tracking
- Agent startup speed has been improved when service monitoring is enabled
- File Access Tracking: Fixed issue on Windows 2008 and later
- Network Services: Japanese Syslog messages and SNMP traps are now correctly logged to the event log and database

**Version 2.92  April 2011**

**New Features:**
- SNMP trap daemon is introduced and logs v1, v2c and v3 SNMP traps either to the event log or the database
- Syslog daemon has been moved from the EventSentry agent into the "Network Services" service, together with the SNMP daemon. Stability as well as reliability have been improved in the new Syslog daemon
- Performance (optional) as well as environment email alerts now include an attached chart which shows recent performance / environmental data
- Management Console: Clicking a computer icon now displays a summary page
- Event Log Monitoring: Insertion string matching can now match empty strings
- Event Log Monitoring: Number of supported custom event logs has been increased to 30
- Service Monitoring: A recurring alert can be configured when a service remains in the "Stopped" state
- Hardware Inventory: Network adapter speed is now collected, and speed changes are logged to the event log
- Hardware Inventory: Addition and removal of Removable drives (e.g. USB drives) are now detected and logged to the event log
- Hardware Monitoring: The S.M.A.R.T. status of physical drives (when supported) is monitored.
- Disk Space Monitoring: Volumes linked to by junction points are now included when disk space alerts are evaluated / generated. Note: Disk space information in web reports does not yet take junction points into consideration
- Process Monitoring: The number of required instances of a process can now be specified
- Print Tracking: Print tracking now works with Vista and later operating systems
- Network Logon Tracking: When capturing "Logon By Type" events, "Audit Success" can now be excluded
- A new HTTP action submits events to web pages via http or https
- The SMTP action dialog now includes a wizard to build email addresses for common email to SMS gateways
- Additional variable support for the Process, Syslog and Snmp action
- Heartbeat Agent: Improved detection of remote agent status

**Bug Fixes:**
- All bug fixes since the initial 2.91 release have been incorporated into version 2.92, additionally:
Hosts configured with multiple NICs that are added to the configuration with just the IP address, will properly determine their group membership.

Print tracking works with Vista, Win7 and Windows 2008

Version 2.91  November 2009

New Features:
- Event Log Monitoring: Filtering capabilities have been improved to allow for insertion string matching, including the ability to interpret insertion strings as numbers, usernames or file names
- Actions: SNMP action now supports v2c and v3 traps
- Service Monitoring: Now collects service account as well as executable, in both alerts as well as reporting
- Service Monitoring: Service history report now shows every service change per line, with easier readability
- Process Tracking: Command line arguments of an active can now be collected
- Logon Tracking: Group information is now collected
- Software Monitoring: Uninstallation events now include same information as installation events
- Software Monitoring: Windows updates are now collected on Vista, Windows 2008 and Windows 7, and more easily searchable in the web reports
- Hardware Monitoring: IP addresses are now collected, and changes updated dynamically in the background
- File Monitoring: Processing of a file's checksum can now be skipped if the size has not changed
- Management Console: Authentication can now be set globally, in addition to being set on a per-group and per-computer level
- Management Console: Computers in AD-linked groups can be sorted.
- Management Console: Notes can now be added to computers
- Environment monitoring: The minimum monitoring interval has been reduced to 5 minutes
- Reporting: Health status of multiple computers can be displayed in a visual health matrix, scalable to display hundreds of computers in a single page
- Reporting: The network status page now allows the customizations of performance counters as well as disks displayed
- Reporting: Reports are more accessible, and can now be accessed from every page
- Reporting: Most pages have been overhauled and improved for improved usability

Performance Enhancements:
- Event Log Monitoring: Filter processing has been improved, resulting in a lower CPU usage
- Checksum generation (File Monitoring, File Access Tracking) has been improved resulting in lower CPU usage

Bug Fixes:
- All bug fixes since the initial 2.90 release have been incorporated into version 2.91.
- Software Monitoring: Duplicate records of software is not longer shown in the software inventory
- Compliance Tracking: Temp file was used even when its maximum size was set to 0 Mb
- Network Status: This feature has been improved to avoid problems with computers missing, being displayed in the wrong group or not showing up at all
- Disk space Monitoring: Alerts for low disk space are no longer generated when the total disk space is less than the alert (hard) limit to begin with
- Hardware Inventory: Virtual machine detection, as well as Hyper-V detection has been improved for more reliability
New Features:

- Vista, Windows 2008 are monitored with new API
- Event Log Backup feature supports .evtx files
- Database Import Utility supports .evtx files
- New NTP monitoring and synchronization feature
- Event Log Filter Timers now support insertion strings for easier setup & more flexibility
- Scripts can now be embedded into the EventSentry configuration and referenced in application schedules & process actions
- Actions: Jabber action supports chat rooms
- Actions: Process action supports time-based termination and more event logging options
- Actions: Fields in SMTP action can now be customized
- Actions: In addition to controlling services, processes can be terminated (with support for insertion strings)
- Actions: Certain actions can track their trigger history in database
- Actions can now be enabled/disabled based on weekday and time of day
- Compliance: New File Access Tracking feature
- Compliance: Account Management Tracking
- Compliance: Successful & Failed network logon tracking
- Compliance: Audit, Domain & Kerberos policy tracking
- Compliance: Trust Relationship tracking
- Compliance: User & Logon Right change tracking
- Compliance: Improved logon tracking to include domain role and indicate administrative logons
- Compliance: Process tracking includes domain role
- Variables can now be assigned to computers in addition to global & groups
- Service Monitoring: Events now distinguish between services and drivers
- File Monitoring: Can detect alternate data streams (ADS)
- Performance Monitoring: Added “between” condition and “divide by # of processors”
- Software Monitoring: Monitors and records system uptime
- Hardware Inventory: Detects more details about the OS (e.g. editions) as well as hardware
- Management Console: Group-Level Inheritance can be blocked on a per-computer basis
- Management Console: Remote update feature now uses threads for much faster update speeds
- Management Console: Added “Quicktools” to execute any application against a remote computer
- Heartbeat Monitor: Can now utilize credentials set on group or computer items
- Heartbeat Monitor: Can notify you via email when the EventSentry agent is not running
- Web Reports: Extremely granular, built-in authentication has been added
- Web Reports: Users can customize their settings in web reports without affecting global profile settings
- Web Reports: Network Status includes switch to only show erroneous machines
- Web Reports: Network Overview shows disk & performance alerts and event log trends
- Web Reports: Network Overview shows overdue reports and most active machines
- Web Reports: Computer Overview includes event log trend, overview and common errors
- Web Reports: Report management has been improved
- Web Reports: Reports support review as well as a report trigger history
- Web Reports: Right-click menu for column headers allows toggling columns
- Web Reports: Maintenance wizard supports deleting multiple computers at once, and much more
- Web Reports: Database usage page shows storage details of database
- Web Reports: Database can now be created and/or updated using the web reports
- Web Reports: Print output has been significantly improved
- Three completely redesigned widgets using the Yahoo Widget Engine

**Bug Fixes:**
- Several bug fixes in the database import utility for importing log files
- Issues with filter times have been resolved
- Filter test feature has been improved
- Event Log Monitoring has been improved for better reliability

**Version 2.81  September 2007**

**New Features:**
- Database Setup Wizard now supports database connection strings and EventSentry Actions as a destination in addition to System DSNs
- Nessus Import Utility and reporting now supports XML files from Nessus v3 as well
- Web Reports: New “Network Status” overview page
- New SMTP engine now supports TLS/SSL connections
- Event Log Backup files can now be automatically compressed
- Line delimiter can now be specified for non-delimited files as well
- Actions now support a limit feature
- Management Console can automatically check for new versions and patches
- Event Log Database Import utility is now called “Database Import Utility” and supports importing delimited and non-delimited log files
- You can now specify a router for a Heartbeat-Enabled group to suppress duplicate alerts when a router goes down
- Hardware inventory can now distinguish between logical and physical CPUs and show more detailed CPU information
- Web Reports: Computer Overview page supports automatic iteration between computers
- Web Reports: Weekly Logon Reports in Logon Tracking
- Web Reports: Ability to email event records and copy event records to the clipboard
- Web Reports: Calendar popup improved on newer browsers

**Bug Fixes:**
- Improved SQL queries drastically improve speed of most searches on the web reports
- Detailed hardware inventory information (NIC, memory, etc.) would sometimes not be recorded correctly
- Host names / IP addresses of remote Syslog hosts would not be included in events or the database if the IP address of the remote host could not be resolved
- Resolved bug in environment monitoring dialog
- Computers logging on to Citrix or Terminal Servers would show up in the “Computers” field of the Logon Tracking page
- Active Directory Auto-Refresh: Computers that were removed from AD would not automatically be removed from the corresponding group
- Web Reports: Improved Correlation between logon and process tracking
- Web Reports: Several bug fixes in combination with MySQL, profile editor

**Version 2.80  May 2007**

**New Features:**
- Log File Monitoring allows you to monitor both non-delimited and delimited files. You can either consolidate content into the database or receive alerts based on text logged to the log files.
- File Monitoring allows you to be notified when files in a monitored directory are changed (includes checksum hashes), and you can either track changes in the database or receive alerts.
- Directory Monitoring alerts you when a monitored directory exceeds a preset size.
- Jabber notifications allow you to send IM notifications, e.g. using Google Talk.
- The hardware inventory feature now includes detailed information about installed memory and available slots, installed network cards, optical drives and you can remotely power on computers using WakeOnLAN.
- Logon Tracking now includes more detailed information such as remote IP address, session connections/disconnections and workstation unlocks.
- The heartbeat agent now supports recurring alerts.
- As always we also fixed minor bugs and optimized various aspects of the agent to continuously increase the availability of the agents.
- Two new wizards were added for the log file monitoring and for setting up thresholds.
- A "filter test" utility has been added that allows you to test events against your filter rules by simply right-clicking an event in the built-in event viewer.
- Insertion Strings of events can now be displayed in the subject of an email ($STR1, $STR2, ...).
- System Health features now include an "Alerts" button to easily create filters for events logged by the respective feature.
- Package summary pages now include description of packages.
- Hardware inventory feature can generate alerts when memory, CPU count or number of installed drives change.

**Bug Fixes:**

- Custom event log settings are now completely transferred to remote machines when pushing the configuration.
- Some events would not be transferred correctly with the SNMP action.
- On 64-bit systems, EventSentry now shows 32-bit and 64-bit installed software.

**Version 2.72 8th September 2006**

**New Features:**

- Remote configuration updates do not require the Remote Registry Service anymore, but instead use the ADMIN$ share. A work-around without the ADMIN$ share exists.
- Remote update shows the total and average time it took to perform an action.
- Event Log Backup Files (.evt) can be imported into the EventSentry database.
- Event Message Browser lets you view and test all installed event messages.
- Two wizards where added to accomplish common tasks.
- Disk space alerts are now cleared after an alert, the volume name is also shown in alerts.
- Disk space web-reports can be filtered/grouped on the group level.
- Speed of performance charts was improved significantly.
- Expanded the "toggle" functionality to most search pages.
- A user-configured IP address will now be used on the web reports.

**Bug Fixes:**

- Deleting a database action could incorrectly configure the notifications of existing health and tracking features, including notifications set on the package-level.
- Remote update would not work correctly when the EventSentry was not installed locally.
- Creating a new package and immediately configuring it to be global would not work.
The automatic configuration backup feature would not correctly delete old files
A temperature-only sensor could not be configure for a position other than 1
The temperature and/or humidity sensor would not work correctly
Remotely connected event logs would sometimes not be restored correctly
Filters and folders with the same name would crash the GUI
The event log summary dialog would display incorrect data when connected to remote hosts
Finding Event IDs works correctly now
Creating multiple SNPP action notifications was not possible
Resolved problems with event reports on SQL Server 2005
Resolved problems with IP address lookup
Resolved problems with the performance reports

Version 2.71 6th July 2006

New Features:
- Filter Timers for event-log relation
- Additional hardware sensors: Motion-, Smoke- and Water sensors
- Nessus reporting support
- Database purge utility (command-line based)
- Installer now supports MySQL
- Agent: New Shutdown/Reboot and Service Control action
- Agent: Support for more runtime variables in SMTP Header/Footer
- Heartbeat Monitoring: Ping tracking
- Heartbeat Monitoring: Maintenance schedule can be accounted for in uptime statistics
- Improved hardware inventory (now also detects serial numbers, model and graphic adapter/resolution)
- Remote Update utility to automate remote update tasks
- Improved dashboard
- Ability to save the configuration as a HTML file
- Maximum temp file size mechanism change
- Various improvements in the web reports

Bug Fixes:
- Pushing the agent to a remote host running the x64 edition Windows Server 2003 would sometimes not work
- Fixed problems with application scheduler that would not execute certain files properly
- Fixed various small bugs in management console application
- Fixed problem with certain threshold settings
- Fixed bug with performance monitoring
- Fixed XSS vulnerability in web reports
- Fixed minor issues in database setup wizard
- Fixed problem with event log backup assignments
- Fixed problem when computers were added with FQDN instead of NetBIOS name

Version 2.70 9th February 2006

New Features:
- Management console now supports filter, health and tracking package for easier and more flexible administration
- NETIKUS.NET offers standard filter and health packages that can be updated directly from the management console over the Internet
- Performance monitoring to track performance information (e.g. CPU usage, memory usage) in a database and/or receive performance alerts via notifications (e.g. email)
Filter packages can be configured to be automatically active when one or more services are installed

Environment monitoring now supports temperature and humidity ranges and also clears previously issued alerts

Pager support for paging providers that support the SNPP protocol

Service monitoring now includes database support, allowing you to query service status, history and uptime through the web reports

Autorun Monitoring is now called “Software Monitoring”

Software inventory is now included as Software Monitoring now includes database support. This allows you to query installed applications and installation history through the web reports.

Software monitoring also monitors the ActiveSetup registry key

3rd Party Application is now called “Application Scheduler” and supports running custom monitoring tasks in a recurring fashion, e.g. every 30 seconds.

Logon tracking monitors logon's and logoffs, enabling you to view detailed logon/logoff information about users through the web reports

Print tracking monitors all print jobs and allows you to see print job data and statistics through the web reports, including the ability to assign cost to print queues for invoicing

The threshold feature has been simplified and offers new features

The built-in event log viewer supports opening .evt files, you can also open .evt files directly from explorer

Remotely connected event logs can automatically be restored after restarting the management console

The remote update computer list can automatically be sorted

Heartbeat agent now supports maintenance schedules that can be set for individual computers and/or groups

Management console supports searching for filters and computers

Management console can automatically backup the entire configuration at preset intervals

The completely redesigned web reports now offer a dashboard, event log reports, a profile editor, a maintenance wizard and much more!

**Bug Fixes:**

- Reduced size of configuration in registry for faster remote updates
- Increased agent stability
- Fixed problems with moving and cutting/pasting filters
- Several problems in the web reports have been fixed
- Duplicate computers cannot be entered anymore and no longer cause problems with the heartbeat agent

**Version 2.60  1st June 2005**

**New Features:**

- SNMP Support (sending traps)
- Monitoring of application installation/uninstallation
- Monitoring of machine-based autorun registry keys and directories
- Web reports now feature an uptime calculation page
- Ping option for remote update can be toggled
- System health options can now be set to block inheritance
- Process Monitoring can be configured to start after X seconds
- Various enhancements in the management application, including proxy server support for feedback and news feature
- Added ping dependency in heartbeat monitoring
- Added additional monitoring options in heartbeat monitoring
• Added database backup feature (if database is temporarily unavailable) to heartbeat monitoring
• Agents installed through remote update can now be uninstalled on target machines using "Add/Remove Programs"
• Desktop action notification now supports remote hosts in addition to the local host
• "Online Configuration Update" feature was improved for higher stability
• Map IP address to alias in remote update
• Changed MSI installer from Wise to InstallShield for higher stability and more future features

Bug Fixes:
• Some SIDs were not resolved to usernames correctly
• Clicking on the "Computers" container would show a wrong path in an error message
• Computers would randomly not show up in the web reports computer list
• Saving the configuration would increase the memory usage on the agent, without freeing it (~200kb)
• Some processes in "Process Tracking" would incorrectly show up as “still running” when they had exited
• Bootscan feature of Process Tracking would not record all activity correctly
• Recurring event filters would not work 100% correctly when a schedule would end exactly at midnight
• SMTP Footer would not appear in Mini Emails
• Under certain circumstances on very busy event logs (e.g. security event log on domain controllers) some event records would be skipped and not processed by EventSentry.
• The EventSentry agent would crash under special circumstances when using the summary notification feature.
• When clearing an event log the EventSentry agent would not continue to monitor this log.
• Fixed various issues with SP1 of Windows Server 2003
• Various bug fixes in the management application
• Various bug fixes in the EventSentry agent
• Fixed problems in combination with DEP (data execution prevention) in SP1 of Windows Server 2003

Version 2.50 26th January 2005

New Features:
• Temperature & Humidity monitoring with external device
• Heartbeat monitoring of remote hosts (ES agent monitoring, PING and TCP port checks)
• Local computername may now be added to remote update list
• ODBC Target supports ODBC connection strings in addition to DSN names for easier deployment
• "Audit Process Tracking" can now also be switched off through "Process Tracking" feature
• Recurring event feature lets you define events that you expect to appear (such as a tape backup) during a certain time period, and become notified if they are not
• Computer field added to event log filter properties
• Event Log Backup feature now supports environment variables in file name
• Event Log Full detection now also supports the ODBC, NET SEND, SYSLOG and DESKTOP actions
• GUI: Event Log Viewer supports sorting
• GUI: Remote Update results window allows for sorting
• GUI: Remote Update also sends computer names
- GUI: Remote Update "Computers" container supports sorting and drag/drop
- GUI: Targets support drag/drop
- GUI: Active Directory linked groups now show the actual computers under the "Computers" container and allow for authentication to be set on a per-host level
- GUIDs in event log records are resolved to display name
- Filter Source, Category and Users allow for multiple values, separated by comma
- Filter Source, Category and Users support negation with exclamation mark
- Binary data of events now also available in all notifications, GUI and web reports
- Additional variable support for the FILE action
- ASP and PHP Web reports now work with all supported databases (Access, MSSQL, MySQL, Oracle), the PHP web reports have been switched to use ODBC
- A new Database Wizard now creates all tables, indexes and permissions automatically on MSSQL, MySQL and Oracle
- The new MSI installer optionally creates a virtual IIS directory and/or sets up the MS SQL Server database automatically
- SMTP action now supports an optional header and footer that can be added to every email
- Service Monitoring: Included/Excluded services now support wildcards
- Process Tracking: Included/Excluded processes now support wildcards

**Bug Fixes:**
- Database layout completely redesigned for faster web reporting
- Event Log Scanning engine significantly improved
- Memory Leak in filter processing removed
- Absolute diskspace limits now work for values > 4Gb
- Selecting a particular set of logical drives would not work
- ASP Web pages corrected to support Access databases without restrictions
- ASP Web pages corrected to support non-US date formats
- Threshold feature incorrectly counting excluded events towards limits
- Filtering of "Filter Text" would not work correctly when filter text attempted to match the last character of an event log record
- Password for group (remote update) not saved correctly
- GUI will not allow more than one instances anymore on computers running Terminal Services to avoid data corruption
- GUI will not freeze while performing remote updates and switching to another application
- Several bug fixes in ASP and PHP web reports
- Unsupported characters were allowed in filter names, resulting in configuration corruption

**Version 2.43  22nd July 2004**

**New Features:**
- Process Tracking records all process activity in a database and allows you to see a process history on all monitored hosts
- Service monitoring can control services and maintain a set status. Failed services can now be automatically restarted
- Disk Space Monitoring allows for more granular settings for warnings and database connections
- Disk Space Monitoring will now recognize when new (fixed) disks are added or removed during runtime
- Event Log Backup allows for backups of all event logs for faster configuration
- Database table names can now be specified for each of the features requiring a database (ODBC action, disk space trend collection and detailed process tracking)
- GUI: "Force News Update" reloads latest news
Bug Fixes:

- GUI: Filters can be commented
- Handle leak in eventsenry_svc.exe.
- Memory leak in NonPaged pool when using the TCP syslog action and remote syslog host is not accepting TCP connections
- Launching applications with the "3rd Party Applications" feature might show error "Invalid access to memory location" and the application would not run.
- An error with the summary notification feature could crash the application when a large amount of events (more than the configured maximum) were summarized.
- Right-Click on SYSTEM event log in tray icon opens security log (no other logs are affected)

Version 2.41 7th June 2004

New Features:

- Added $HOSTNAME variable to event log backup feature

Bug Fixes:

- Warning messages in PHP interface removed
- Wrong $DAY, $MONTH and $YEAR variables in event log backup feature
- OLE DB error in index.asp file removed when using an MS Access database

Version 2.40 25th May 2004

Version 1.x Compatibility mode will no longer be supported starting with Version 2.40 of EventSentry. If you are still running 1.x agents in your network then you will need to upgrade them to version 2.40.

New Features:

- GUI: Tree in navigation pane restructured for easier navigation, general usability improvements
- GUI: Maximum groups, actions were increased
- GUI: Active Directory Import (with "Link" feature) added
- GUI: Up to 5 remote event logs can be added to navigation pane
- GUI: Change detection added, GUI tries to determine whether changes were made and only prompts to save then
- GUI: Event Log Viewer filter added (filter for errors, warnings, information, audit success & failure)
- GUI: Only active group is sent to remote computers with remote update
- GUI: One-Button remote agent installation
- GUI: Tree status is now also saved/restored when connecting to remote computers
- GUI: ODBC action has a test button now too
- SMTP Target: Mini-Emails can now be customized
- SMTP Target: Dial RAS connections before sending emails
- SYSLOG Target: This action has been optimized and should offer higher throughput
- Custom variables are introduced, variable processing improved
- Variable $EVENTMESSAGE for SMTP subject added
- Automatically backup and clear event logs on a regular basis
- Run command-line applications and log their output to the event log
- Monitor memory consumption of processes to detect possible memory leaks
- Monitor diskspace, including trend change detection
- Trial Version & Full Version are now one product

Bug Fixes:

- GUI: Remote Update: Health settings of a group could be deleted when only updating filters
• GUI: Service Monitoring would not save changes when adding services that don't exist on local machine
• GUI: Feedback forms do not disappear when connection was unsuccessful
• GUI: Renaming groups could yield random results
• SERVICE: Filter processing has been optimized
• SERVICE: Some boot time events could be ignored
• SERVICE: Formatting of event log records has been corrected and improved
• SERVICE: SMTP message now contain a Message ID

Removed Features:
• 1.x Compatability Mode was removed. If you are upgrading from version 1.x then you will need to upgrade to version 2.30 first to preserve existing filters.

Version 2.30 3rd December 2003

New Features:
• EventSentry now monitors services
• Small enhancements in the management interface
• Filter Groups are now referred to as “Groups”
• Filter Groups can be added/removed in Remote Update, System Health and Filters tree
• PHP version of web interface added (ASP + PHP now supported)
• Added links to eventid.net, google, etc. to web files
• Syslog facility/level now mapped to event category for incoming syslog packets

Bug Fixes:
• Long date format problem in event viewer resolved
• Rename problem in GUI resolved
• Import Problem in GUI resolved

Version 2.21 5th November 2003

New Features:
• Syslog target now supports TCP in addition to UDP
• Remote Update speed improved
• Remote Update displays more informative error messages
• Remote Update now supports different credentials
• Added troubleshooting section in help file and GUI for every target
• Numerous enhancements in the management application
• Added EventSentry Quickstart Guide

Bug Fixes:
• Event records containing a single dot per line could cut off email
• Potential problems in wildcard feature
• Problem in built-in Event Log viewer with certain events resolved

Version 2.20 8th September 2003

New Features:
• (X)HTML emails are sent in multi part/alternative including a non-HTML version of the content. This is useful for email clients that are not capable of displaying HTML messages and for filtering (rules) in MS Outlook
• Wildcard support for filters was added
• The following additional variables for the SMTP target were included: $EVENTSOURCE, $EVENTCATEGORY, $EVENTTYPE, $EVENTID
• The $HOSTNAME variable is now supported in the SMTP Sender email field
• The built-in event log viewer allows you to query web sites to obtain information on a particular event
Bug Fixes:

- Installer features (Management package) improved
- The syslog hostname (as logged & reported by the syslog daemon) was truncated
- The welcome screen might show an invalid event log summary when connected to a remote machine
- Day/Time summaries are sometimes not read correctly on the fly, a service restart is necessary
- Changing the debug logging level requires a service restart
- Various improvements in the management application

Version 2.11  18th August 2003

New Features:

- A customizable Welcome Screen shows important information such as EventSentry news, event log summary and more
- Display speed of the built-in event viewer was greatly improved
- Invalid filter order is detected by management interface
- For better usability some menu options were renamed
- Sample ASP pages for querying an ODBC database were added
- On German Operating Systems EventSentry logs German messages to the event log

Bug Fixes:

- The service (agent) underwent a major security code review
- Memory usage was reduced and optimized
- Exclude filters using more than one target would not exclude events properly
- Drag & Drop would sometimes not work properly
- Creating filters or targets would fail when clicking with mouse instead of hitting enter
- Remote Update would sometimes not connect to certain machines
- Import Wizard would only import ~250 computers
- Size & positioning issues with desktop notification feature were corrected
- Potential problems in the network target have been resolved
- Problems with the summary notification have been resolved

Version 2.10  3rd July 2003

New Features:

- Custom event logs can now be managed and monitored

Bug Fixes:

- Fixed problems in the built-in event viewer and other minor problems

Version 2.01  18th June 2003

New Features:

- Added check box functionality for remote update
- All groups can now be updated at once

Bug Fixes:

- Fixed problems in the remote update feature (including service installation)
- Fixed problems in built-in Event Viewer

Version 2.00  5th June 2003

New Features:

- Added installer software
- Completely redesigned the management interface (GUI)
- Filters can be assigned to multiple targets
Support, FAQ, Version History

- Smtp target enhancements
- Added network target (ala net send)
- Added process target
- Added sound target
- Added desktop target

**Bug Fix:**
- Permanent summary notification on Windows NT4 might not work due to missing %TEMP% variable

**Version 1.15  11th March 2003**

**New Features:**
- Summary features events are now stored throughout service restarts
- Filter option "Filter Text" is not case sensitive anymore

**Bug Fixes:**
- "Stop processing other filters" didn't work in combination with summary feature under some circumstances
- Other minor bug fixes

**Version 1.14  25th February 2003**

**New Features:**
- Targets can now be enabled/disabled
- Multiple concurrent instances of the GUI are prevented

**Bug Fixes:**
- The "stop processing other filters" option didn't work correctly under some circumstances
- Bootscan would report too many events under some circumstances
- Using ODBC with a MS SQL Server would sometimes not write events to the database
- Excluding filters for particular targets would under some circumstances not work

**Version 1.12  10th February 2003**

**Bug Fixes:**
- The filter summary dialog box is cleared/reset under some circumstances
- A filter group update does not correctly set the active filter group on the target computer
- Sending emails with certain mail servers would fail

**Version 1.10  4th February 2003**

**New Features:**
- Introduced filter groups (see help for an explanation)
- Added the parallel ASCII-printer target
- Added email importance flags
- Added/improved computer list import/export
- Added GUI tips

**Bug Fixes:**
- A special kind of event log entry could crash the service
- Database DATETIME field was not used (text was used instead)
- Event log entries would sometimes be ignored
- Fixed GUI ALT-F4 issue.
- Other minor fixes in both GUI and service
Version 1.03  16th January 2003

New Features:
- Added the $HOSTNAME variable for the SMTP subject and FILE filename, added HTML customization options.

Bug Fix:
- If an event log is configured to "overwrite events as needed" and events are being overwritten (because the event log is full) then EventSentry can stop monitoring this particular event log under certain circumstances.

Version 1.02  22nd December 2002

Bug Fix:
- Under some circumstances the GUI could crash when performing any kind of batch update.
- The EventSentry service is not affected by this problem.

Version 1.00  19th December 2002
This was the initial public release of EventSentry.

8.3.1  Version Numbering System

This page explains how version numbers for EventSentry are created. A typical EventSentry version looks like this:

3.4.1

3  Major Release Number  This number is increased when EventSentry undergoes a major change, such as the introduction of the new web reports in v3.

.  Separator

4  Minor Release Number  This number is increased when a new feature is introduced such as the support for log file monitoring.

1  Sub-Release Number  This number is increased when minor features have been added and bugs have been fixed.
9 Suggestions and Future Features

Future Features
There are many product enhancements planned for EventSentry. Please review our online roadmap for up-to-date information on future features and features under development.

In addition, EventSentry is constantly under review to resolve possible problems and improve and tweak existing features. If you have other suggestions please click here.

Suggestions
EventSentry is constantly being reviewed and improved and we have implemented many features from customer suggestions in the past!

If you are missing a feature and would like to see it in a future release then please either start a discussion in our Feature Requests forum or fill out a feedback form in the Feedback menu and include all or some of the following information:

- A description of the feature
- Why and how this feature would benefit you
- An example

After looking through your request we will get back to you and let you know if and when we will add your feature to EventSentry.

10 Credits

Beta Testers
We would like to thank all the individuals who helped us beta test EventSentry. We received many suggestions, ideas, and bug reports that enabled us to make EventSentry a better and more stable product.

Bug Discoverers
We thank everybody who took the time to report problems and/or bugs in EventSentry.

Suggestions
Many thanks to all individuals who sent us suggestions. We have implemented countless customer suggestions over the past years.

Development
We would like to thank Chris Maunder and others from CodeProject for providing sample classes. Many thanks to PJ Naughter, for the many MFC libraries he provides to the community. Many thanks to Stephan Brumme for Fast CRC32.

Individuals
Many thanks to Dina, Dieter, Juergen, Mariano, Dietward, Urban, Bud, Rick and Josh who are and have been helping us make EventSentry better, better and better!

Translations
Many thanks to Mihai, Eduardo and Jupiter Technology for helping us translate the web reporting into additional languages.

Projects
EventSentry uses components / software from the following projects:
10.1 PostgreSQL

PostgreSQL is released under the PostgreSQL License, a liberal Open Source license, similar to the BSD or MIT licenses.

PostgreSQL Database Management System
(formerly known as Postgres, then as Postgres95)

Portions Copyright © 1996-2019, The PostgreSQL Global Development Group

Portions Copyright © 1994, The Regents of the University of California

Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

10.2 PostgreSQL ODBC

PSQLODBC.DLL - A library to talk to the PostgreSQL DBMS using ODBC.
Copyright (C) 1998 Insight Distribution Systems
Copyright (C) 1998 - 2011 The PostgreSQL Global Development Group

Multibyte support was added by Sankyo Unyu Service, (C) 2001.

The code contained in this library is based on code written by
Christian Czezatke and Dan McGuirk, (C) 1996.

This library is free software; you can redistribute it and/or modify
it under the terms of the GNU Library General Public License as
published by the Free Software Foundation; either version 2 of the
License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Library General Public License for more details.

You should have received a copy of the GNU Library General Public
License along with this library (see "license.txt"); if not, write to
the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA
02139, USA.

How to contact the authors:

email:   pgsql-odbc@postgresql.org
website: http://pgfoundry.org/projects/psqlodbc

**********************************************************************

10.3 Qt

EventSentry uses software from the Qt GUI Toolkit (v5.1x). The Qt source code used in EventSentry can
be downloaded from here.

The Qt GUI Toolkit is Copyright (C) 2015 The Qt Company Ltd.
Contact: http://www.qt.io/licensing/

Qt is available under the LGPL.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]
Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary
General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for
making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) The modified work must itself be a software library.
   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.
In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit
modification of the work for the customer's own use and reverse
engineering for debugging such modifications.
You must give prominent notice with each copy of the work that the
Library is used in it and that the Library and its use are covered by
this License. You must supply a copy of this License. If the work
during execution displays copyright notices, you must include the
copyright notice for the Library among them, as well as a reference
directing the user to the copy of this License. Also, you must do one
of these things:

a) Accompany the work with the complete corresponding
machine-readable source code for the Library including whatever
changes were used in the work (which must be distributed under
Sections 1 and 2 above); and, if the work is an executable linked
with the Library, with the complete machine-readable "work that
uses the Library", as object code and/or source code, so that the
user can modify the Library and then relink to produce a modified
executable containing the modified Library. (It is understood
that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application
to use the modified definitions.)
b) Use a suitable shared library mechanism for linking with the
Library. A suitable mechanism is one that (1) uses at run time a
copy of the library already present on the user's computer system,
rather than copying library functions into the executable, and (2)
will operate properly with a modified version of the library, if
the user installs one, as long as the modified version is
interface-compatible with the version that the work was made with.
c) Accompany the work with a written offer, valid for at
least three years, to give the same user the materials
specified in Subsection 6a, above, for a charge no more
than the cost of performing this distribution.
d) If distribution of the work is made by offering access to copy
from a designated place, offer equivalent access to copy the above
specified materials from the same place.
e) Verify that the user has already received a copy of these
materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the
Library" must include any data and utility programs needed for
reproducing the executable from it. However, as a special exception,
the materials to be distributed need not include anything that is
normally distributed (in either source or binary form) with the major
components (compiler, kernel, and so on) of the operating system on
which the executable runs, unless that component itself accompanies
the executable.

It may happen that this requirement contradicts the license
restrictions of other proprietary libraries that do not normally
accompany the operating system. Such a contradiction means you cannot
use both them and the Library together in an executable that you
distribute.

7. You may place library facilities that are a work based on the
Library side-by-side in a single library together with other library
facilities not covered by this License, and distribute such a combined
library, provided that the separate distribution of the work based on
the Library and of the other library facilities is otherwise
permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work
based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this license. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this license to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the
original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the
"copyright" line and a pointer to where the full notice is found.
   <one line to give the library's name and a brief idea of what it does.>
   Copyright (C) <year>  <name of author>
   This library is free software; you can redistribute it and/or
   modify it under the terms of the GNU Lesser General Public
   License as published by the Free Software Foundation; either
   version 2.1 of the License, or (at your option) any later version.
   This library is distributed in the hope that it will be useful,
   but WITHOUT ANY WARRANTY; without even the implied warranty of
   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
   Lesser General Public License for more details.
   You should have received a copy of the GNU Lesser General Public
   License along with this library; if not, write to the Free Software
   Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301  USA

Also add information on how to contact you by electronic and paper mail.
You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:
   Yoyodyne, Inc., hereby disclaims all copyright interest in the
   library 'Frob' (a library for tweaking knobs) written by James Random Hacker.
   <signature of Ty Coon>, 1 April 1990
   Ty Coon, President of Vice
   That's all there is to it!

10.4 GeoIP

This product includes GeoLite2 data created by MaxMind, available from http://www.maxmind.com.

10.5 cgminer

EventSentry uses code from the cgminer project to calculate sha256 checksums.

   * FIPS 180-2 SHA-224/256/384/512 implementation
   * Last update: 02/02/2007
   * Issue date: 04/30/2005
   *
   * Copyright (C) 2013, Con Kolivas <kernel@kolivas.org>
   * Copyright (C) 2005, 2007 Olivier Gay <olivier.gay@a3.epfl.ch>
   * All rights reserved.
   *
   * Redistribution and use in source and binary forms, with or without
   * modification, are permitted provided that the following conditions
   * are met:
   * 1. Redistributions of source code must retain the above copyright
      notice, this list of conditions and the following disclaimer.
   * 2. Redistributions in binary form must reproduce the above copyright
      notice, this list of conditions and the following disclaimer in the
      documentation and/or other materials provided with the distribution.
   * 3. Neither the name of the project nor the names of its contributors
      may be used to endorse or promote products derived from this software
      without specific prior written permission.
   *
   * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS `AS IS' AND
   * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
   * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
10.6 RapidJSON

Copyright (C) 2015 THL A29 Limited, a Tencent company, and Milo Yip. All rights reserved.

If you have downloaded a copy of the RapidJSON binary from Tencent, please note that the RapidJSON binary is licensed under the MIT License.

If you have downloaded a copy of the RapidJSON source code from Tencent, please note that RapidJSON source code is licensed under the MIT License, except for the third-party components listed below which are subject to different license terms. Your integration of RapidJSON into your own projects may require compliance with the MIT License, as well as the other licenses applicable to the third-party components included within RapidJSON. To avoid the problematic JSON license in your own projects, it's sufficient to exclude the bin/jsonchecker/ directory, as it's the only code under the JSON license.

A copy of the MIT License is included in this file.

Other dependencies and licenses:

Open Source Software Licensed Under the BSD License:

The msinttypes r29
Copyright (c) 2006-2013 Alexander Chemeris
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS AND CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Open Source Software Licensed Under the JSON License:

json.org
Copyright (c) 2002 JSON.org
All Rights Reserved.

JSON_checker
Copyright (c) 2002 JSON.org
All Rights Reserved.

Terms of the JSON License:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

The Software shall be used for Good, not Evil.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Terms of the MIT License:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
10.7 Google Protocol Buffers

Copyright 2008 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

   * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
   * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
   * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

10.8 PCRE

PCRE LICENCE
------------

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself. The data in the testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.
THE BASIC LIBRARY FUNCTIONS
-----------------------------

Written by: Philip Hazel
Email local part: ph10
Email domain: cam.ac.uk

University of Cambridge Computing Service,

Copyright (c) 1997-2016 University of Cambridge
All rights reserved.

PCRE JUST-IN-TIME COMPILATION SUPPORT
----------------------------------------

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu

Copyright (c) 2010-2016 Zoltan Herczeg
All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER
--------------------------------

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu

Copyright (c) 2009-2016 Zoltan Herczeg
All rights reserved.

THE C++ WRAPPER FUNCTIONS
-----------------------------

Contributed by: Google Inc.

Copyright (c) 2007-2012, Google Inc.
All rights reserved.

THE "BSD" LICENCE
-----------------

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

10.9 Zlib

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.
10.10 Boost

Boost Software License - Version 1.0 - August 17th, 2003
http://www.boost.org/users/license.html

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

10.11 Crypto++

Compilation Copyright (c) 1995-2016 by Wei Dai. All rights reserved. This copyright applies only to this software distribution package as a compilation, and does not imply a copyright on any particular file in the package.

All individual files in this compilation are placed in the public domain by Wei Dai and other contributors.

I would like to thank the following authors for placing their works into the public domain:

Joan Daemen - 3way.cpp
Leonard Janke - cast.cpp, seal.cpp
Steve Reid - cast.cpp
Phil Karn - des.cpp
Andrew M. Kuchling - md2.cpp, md4.cpp
Colin Plumb - md5.cpp
Seal Woods - rc6.cpp
Chris Morgan - rijndael.cpp
Paulo Baretto - rijndael.cpp, skipjack.cpp, square.cpp
Richard De Moliner - safer.cpp
Matthew Skala - twofish.cpp
Kevin Springle - camellia.cpp, shacal2.cpp, ttmac.cpp, whrlpool.cpp, ripemd.cpp
Ronny Van Keer - sha3.cpp

The Crypto++ Library (as a compilation) is currently licensed under the Boost Software License 1.0.

10.12 WinPCAP

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.
This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.
This product includes software developed by Yen Yen Lim and North Dakota State University.


Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors."

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED `AS IS' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 1995, 1996, 1997 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the Kungliga Tekniska Högskolan and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1997 Yen Yen Lim and North Dakota State University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by Yen Yen Lim and North Dakota State University"
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright (c) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1996 Juniper Networks, Inc. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution. The name of Juniper Networks may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 2001 Daniel Hartmeier All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright 1989 by Carnegie Mellon.

Permission to use, copy, modify, and distribute this program for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Carnegie Mellon not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Carnegie Mellon and Stanford University. Carnegie Mellon makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

**10.13 Tomcat, Play! Framework**

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.
2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside
or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

10.14 jQuery

Copyright JS Foundation and other contributors, https://js.foundation/

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

10.15 OpenJDK JRE

GNU General Public License, version 2, with the Classpath Exception

The GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free
Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

© <2002 - 2022> ... NETIKUS.NET ltd
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise
the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus
excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

"CLASSPATH" EXCEPTION TO THE GPL

Certain source files distributed by Oracle America and/or its affiliates are subject to the following clarification and special exception to the
GPL, but only where Oracle has expressly included in the particular source
file's header the words "Oracle designates this particular file as subject
to the "Classpath" exception as provided by Oracle in the LICENSE file that
accompanied this code."

Linking this library statically or dynamically with other modules is
making a combined work based on this library. Thus, the terms and
conditions of the GNU General Public License cover the whole combination.

As a special exception, the copyright holders of this library give you
permission to link this library with independent modules to produce an
executable, regardless of the license terms of these independent modules,
and to copy and distribute the resulting executable under terms of your
choice, provided that you also meet, for each linked independent module,
the terms and conditions of the license of that module. An independent
module is a module which is not derived from or based on this library. If
you modify this library, you may extend this exception to your version of
the library, but you are not obligated to do so. If you do not wish to do
so, delete this exception statement from your version.