

EventSentry Overview

Part I About This Guide	1
Part II Overview	2
Part III Installation & Deployment	4
1 Installation with Setup	5
2 Management Console	6
3 Configuration	7
4 Remote Update	10
Part IV Monitoring Architecture	12
1 MSP Architecture	14
Part V EventSentry Components	16
Part VI Heartbeat Monitoring	17
Part VII Event Log Consolidation	19
Part VIII More Information	21

1 About This Guide



Thank you for choosing EventSentry for your event log, system and network monitoring needs. This document has been designed for users to gain a quick understanding of how EventSentry works. We highly encourage you to take 10 minutes to read this document before you start working with EventSentry.



For more information on EventSentry, please read the official help file that comes with EventSentry . The complete help file can also be found at <http://www.eventsentry.com>.

This overview covers the following topics:

- [Brief Overview](#)
- [Installation & Deployment](#)
- [Monitoring Architecture](#)
- [Heartbeat Monitoring](#)
- [Event Log \(Database\) Consolidation](#)

2 Overview

EventSentry is a Windows versatile monitoring suite that monitors event logs, log files, system health, Active Directory and NetFlow. The application consists of the following main components:

- Management Console
- EventSentry Agent
- Heartbeat Agent
- Network Services
- Collector
- Web Reporting

Management Console

The management console does not perform any monitoring and is only used to install, setup and configure the agents on the local and/or remote machines. The management application can be installed on as many machines as you obtained licenses, although one or two installations per network are usually sufficient. You can also launch the management application any computer by running the eventsentry_gui.exe file. [Click here](#) for an overview of the Management Application.

Event Log, Log File, System Health & Compliance Agent

The EventSentry agents run as a Windows service and are not dependent on the management console. Once the agent is configured by the management console it will run silently in the background as a service, and will monitor the event logs and system health according to your configuration.

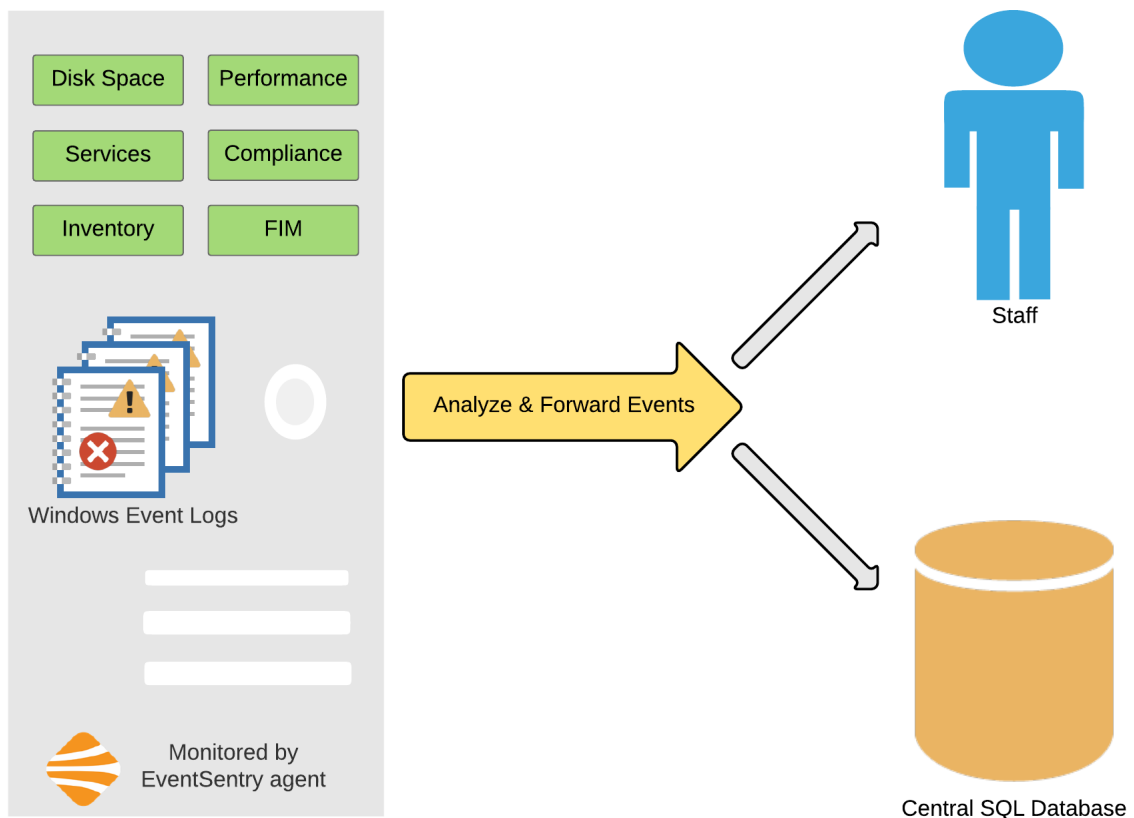


Figure 1



When monitoring Windows-based hosts, then the agent must be installed on every computer that is being monitored.

Heartbeat Agent

The EventSentry heartbeat agent monitors the availability of remote hosts through ping (ICMP) and TCP connections as well as the status of the EventSentry event log agents. The heartbeat agent also polls Non-Windows devices via SNMP GET requests to obtain SNMP counters.

Network Services

The "EventSentry network services service" includes the Syslog, SNMP trap, Netflow and ARP watch daemon. Non-Windows hosts (e.g. Unix, Linux) and network devices send Syslog messages and SNMP traps to this service.

Collector

The collector service enables a 3-tier architecture between an action (e.g. database, email server) and the EventSentry agents, which allows the remote agents to transmit all data securely and reliably. The collector supports compression and secure data transmission via TLS encryption. The collector is optional, without it the agents communicate directly with the respective actions (e.g. database).

EventSentry ADMonitor

Monitors a Active Directory domain (and optionally sub domains) for all object and Group Policy changes and provides a list of all user accounts as well as password reminder emails. ADMonitor also includes additional tools to query AD data natively without requiring the web reports.

Web Reports

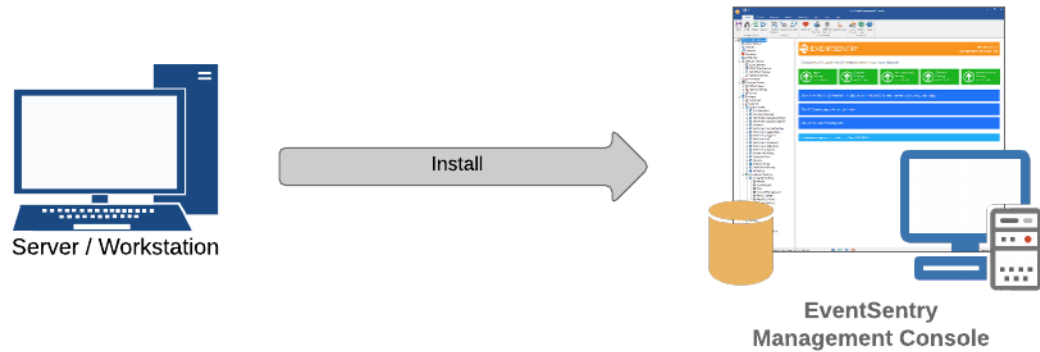
The web-based reporting provides a visual interface to the collected log and system health data. It provides:

- A variety of dashboards and network status overview pages
- Summary views of all collected data (Event log, log files, compliance data, ...)
- Detailed search pages
- Trend graphs for performance, disk space and environment data
- Software and hardware inventory pages
- Scheduled reporting with HTML, PDF, CSV and other output options

3 Installation & Deployment

The diagram below shows the typical steps involved when installing EventSentry on a network:

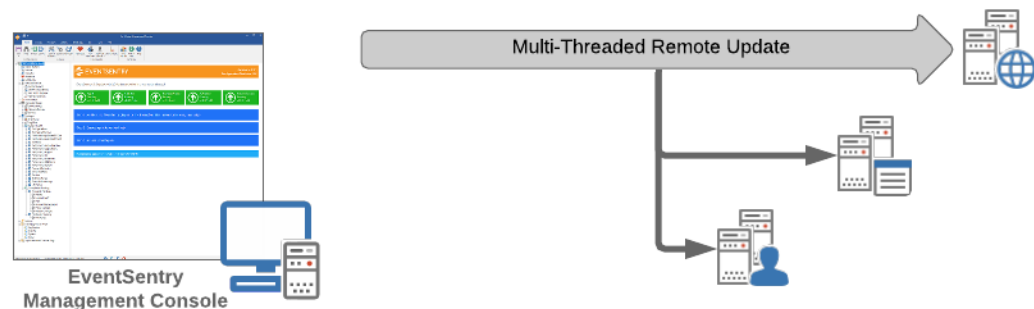
1. Install EventSentry with Setup



2. Configure EventSentry

- 1. Import computers into one or more groups**
AD import, network scan, ...
- 2. Review tutorials and screen casts**
www.eventsentry.com -> Support
- 3. Customize Configuration**
Suppress alerts, tweak intervals
- 4. Setup Syslog or SNMP trap forwarding**
Optional, non-Windows hosts only

3. Deploy Agents




3.1 Installation with Setup

Customers who purchase EventSentry can download the latest version from our secure website at <https://store.netikus.net/account>.

To download the free version of EventSentry, EventSentryLight, [click here](#). Once you have downloaded the setup file you can start the installation by executing the setup file.


Please pay close attention to the installation process as the setup program also initially configures EventSentry for you.


Please note that you will **not** have to run the setup procedure on every host on which you wish to install EventSentry. Use the **remote update** feature to install the EventSentry agent on multiple machines. You can access the **remote update** feature by right-clicking the **Computers** container of each group.



EVENTSENTRY
v3.2


New Features in v3.2

- ▶ 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.
- ▶ 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
- ▶ Additional language support for French, Dutch, Spanish, Polish, Portuguese and Italian
- ▶ Web Reports: Out-of-the-box compliance reports for PCI-DSS, FISMA, Sarbanes Oxley, HIPAA and GLBA
- ▶ Web Reports: Improved & faster performance trend reporting with ability to display multiple trend charts on a single page
- ▶ Web Reports: New Bulk assignment for easier report management
- ▶ Web Reports: Report jobs can be saved to a folder
- ▶ Web Reports: Improved host inventory page now shows switch port (if available), USB version and VM hosts (if available)
- ▶ Web Reports: Health matrix displays computer notes
- ▶ Web Reports: Improved usability throughout
- ▶ Web Reports: Improved connection pool support

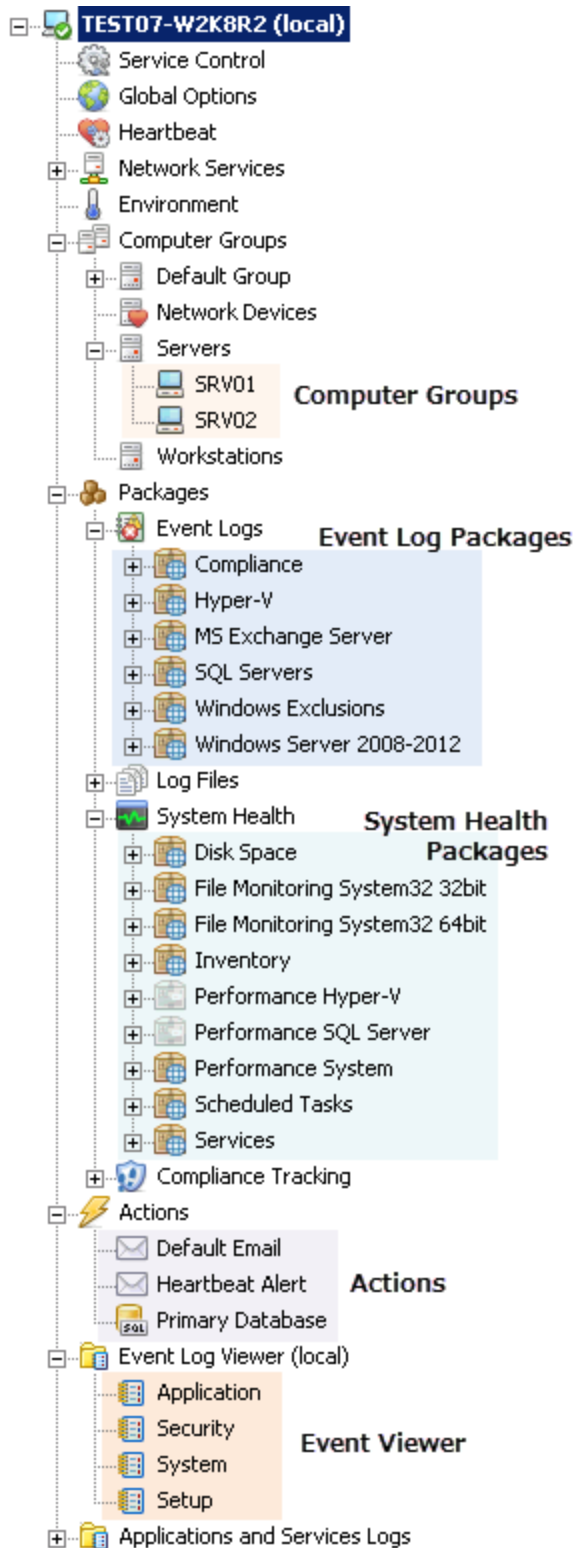

Maintenance
Expires 2017-02-21


Full Installer
Download v3.2.1.0
Important Upgrade Information


Web Reports only
Windows
Linux x86 Linux x64


Archive
Version 3.1 [Download](#)

3.2 Management Console



All features are configured with the EventSentry management console. You can launch the management console by clicking on the EventSentry **Management** icon on the desktop or Programs Folder, or by launching the file **eventsentry_gui.exe**.

Computer Groups

Contains all monitored hosts, including servers, workstations and network devices, with the group icon reflecting the type of the group. EventSentry supports many different group types, including regular groups, ActiveDirectory-integrated, heartbeat-only groups and remote update groups.

Packages

The main configuration is performed with packages, and EventSentry distinguishes between Event Log, Log File, System Health and Compliance Tracking packages.

Some package type only apply to Windows (e.g. Event Log, Log Files, Compliance Tracking), where as some System Health objects (e.g. disk space, inventory, processes) apply to Non-Windows hosts as well.

Actions

Actions is where EventSentry will send collected data an alerts. Most configured packages usually reference one or more actions.

Event Viewer

The built-in event viewer is a light-weight event viewer which can help create and test event log filter rules, and also includes some features not found in the Windows event viewer.

3.3 Configuration

A Minimal Configuration

The most basic EventSentry configuration must include the following:

- One Action
- One Group
- One Event Log Package
- One Installed Agent
- One Management Console

Do-It: Creating A Minimal Configuration

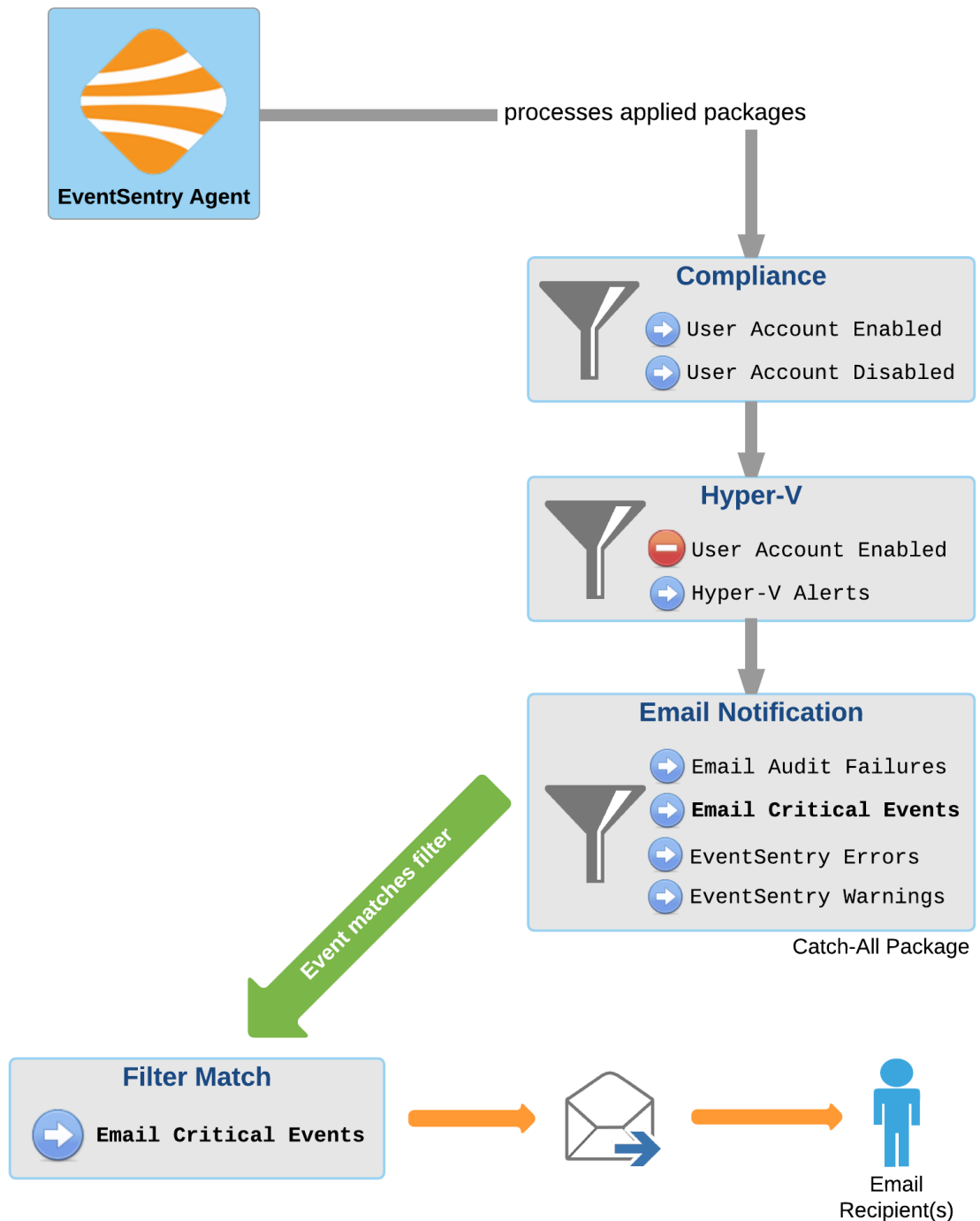
If you specify the SMTP configuration during the setup procedure then the EventSentry installer will automatically create a default configuration consisting of:

- One group (*Default Group*)
- Example event log, log file, system health and compliance tracking packages
- One action (*Default Email*)

Once you have completed the configuration of EventSentry, you can either click the save button in the toolbar or select "Save" from the "File" menu. Remember that configuration changes will *not* become effective until you **save the configuration**.

How do Filters and Actions work?

Filters and event log packages are the core component of EventSentry and determine which events are processed. When EventSentry receives notification of the new event it will process it according to the configured filters and actions (continued from figure 1):



For every event written to any of the monitored event logs, the agent processes all filters of all assigned packages. If the agents finds a match, then the event will be forwarded to the configured notifications. If it does not, then the agent simply ignores/drops the event log record. In the example above, the event record is not matched by any of the exclude filters, but matches the **Email Critical Events** filter and is forward to an email notification.

Configuring EventSentry

You have full control over the configuration of the agent because the configuration is not permanently saved until you click the save button or choose the "Save" option from the "File" menu. Also, EventSentry does not automatically update the configuration of the remote agents; instead, you use the **Remote Update** feature to send the configuration and configuration changes to the agents on your network.

The EventSentry configuration is stored in the registry under the key **HKEY_LOCAL_MACHINE\Software\netikus.net\EventSentry**. Whereas the management application reads and writes the configuration to and from the registry, the agent mostly only reads the configuration from the registry.

3.4 Remote Update

You can use **Remote Update** to manage EventSentry installations on your network. This feature allows you to perform the following tasks **on remote computers**:

- Install, update and uninstall EventSentry agents
- Query the EventSentry status
- Push configuration changes (System Health Settings, Filters, Actions etc.) to remote computers
- Control the EventSentry service (start & stop)

The most commonly used EventSentry options of remote update are explained below:

1. **Deploy Agent:** This will install the agent on the remote computer, copy the local configuration to the remote computer and start the agent.
2. **Update Configuration:** If a computer already has the agent installed then you can use this option to keep the configuration on the remote host up-to-date. "Push Configuration" pushes the entire configuration to the remote computers.
3. **Other Actions -> Update/Upgrade:** After you have installed a new version of EventSentry on the machine with the management application, you can use this option to distribute this new version to all the computers in your network running the EventSentry agent.

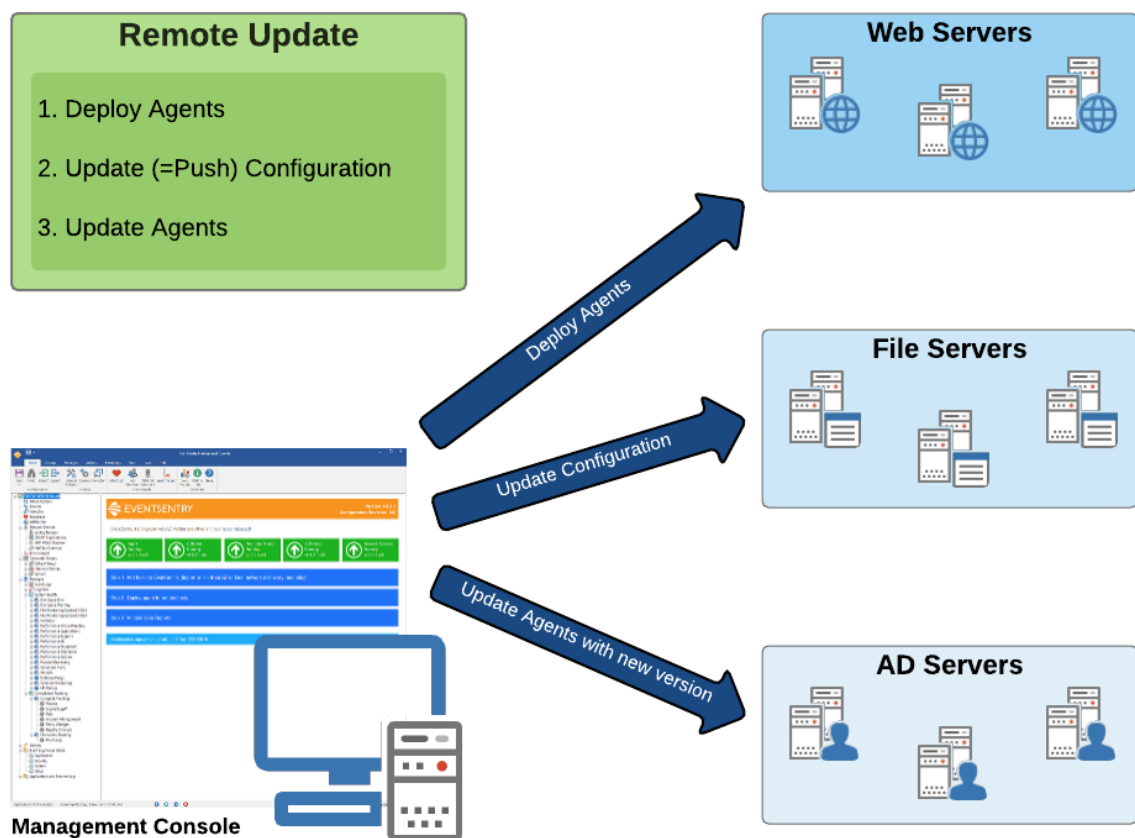


Figure 7

Groups and Remote Update

You can organize your servers into different groups and assign different packages to each group or computer. You can also make packages global, and any package can be blocked on a per-host basis. You can also assign packages based on services that exist on a monitored host.

Do-It: Importing/Adding Computers into Remote Update

Before you can use the remote update you will need to:

1. Make sure one or more groups exist (and add one or more if necessary)
2. **Import** or **manually add** computers to the Remote Update groups

Create Groups: Right-click the **Groups** node and select "Add Group" to add up to 254 groups. The groups you are adding will show up under the **Groups** node immediately.

Manually Add Computers: Right-click the **computers** node under the **group** node and select "Add" from the menu. You can now enter the computer name and hit ENTER to confirm. Repeat this step for every computer you would like to add.

Import Computers: Instead of adding computers one-by-one, you can import computers from either the **network neighborhood**, **active directory** or an **ASCII text file**. Right-click a group and select "Import Computers" to start the import wizard, ASCII files need one computer name per line.

Do-It: Install EventSentry on a number of computers

After configuring actions, filters and adding computers to the remote update list, you are ready to install the EventSentry agent on the remote computers.

1. Right-click a **computers** node and select **Deploy Agent**. If you see check boxes next to the computers then you need to right-click anywhere and select **Go** from the menu.
2. If you would like to install the agent only on a number of computers, then you can right-click the **Computers** container and select **Use Check boxes**.



Hint: Instead of only updating computers from a particular group, you can apply updates to computers from all groups through the "Remote" menu.

Do-It: Updating the EventSentry configuration on a number of computers

If you already installed the agent on all required computers on your network then you can easily update their configuration (system health, actions, filters, etc.) with one simple step. Right-click the **Computers** container of the desired group and select **Push Configuration**. Then select the configuration options you would like to update. After clicking OK, the updated configuration will be sent to the remote computers; a service restart is not necessary.

4 Monitoring Architecture

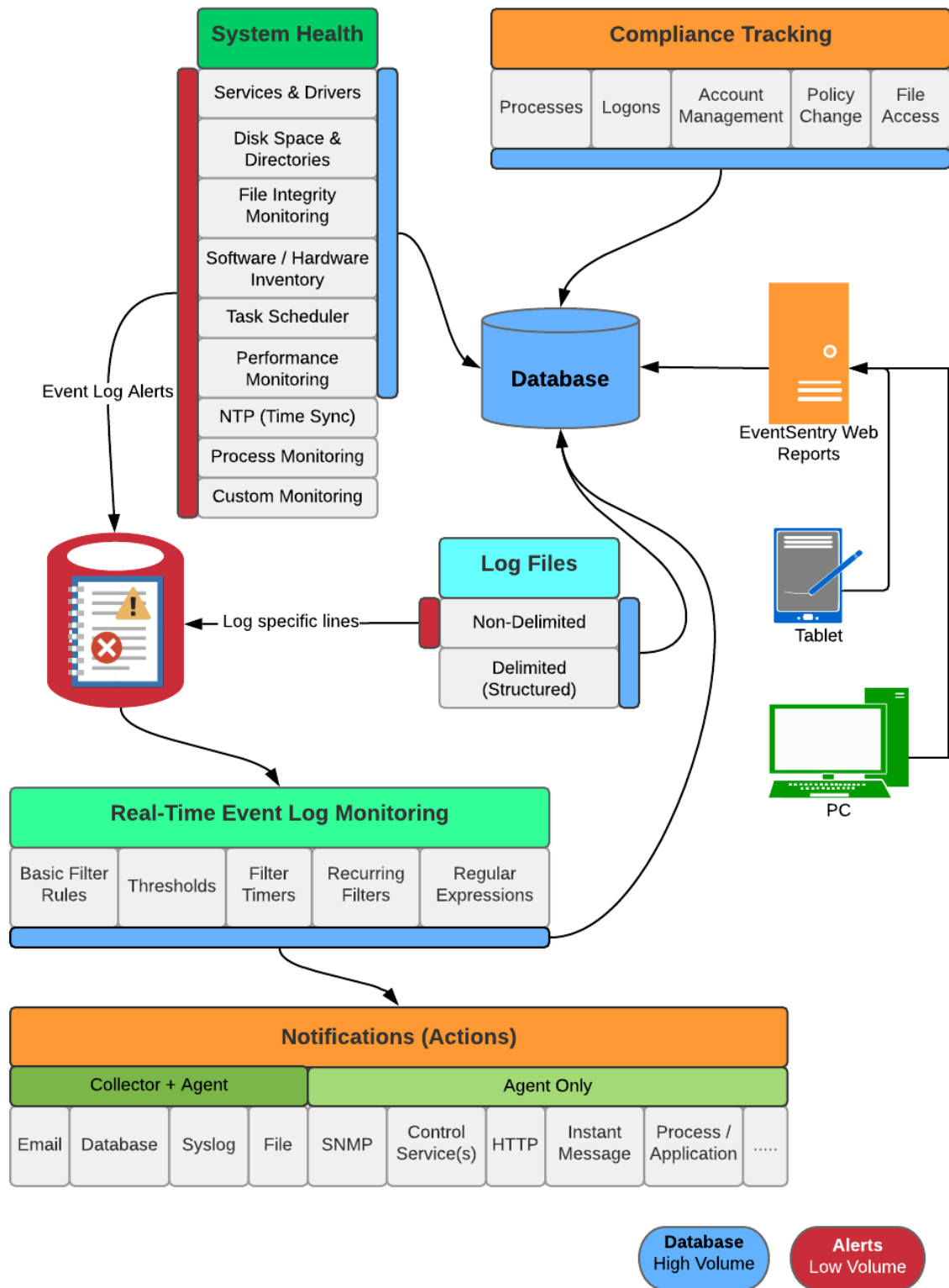
The diagram below shows how the individual components inside the EventSentry agent either alert and/or collect information in the database. The agent includes the following 4 major monitoring components:

1. Event Log Monitoring
2. System Health Monitoring
3. Log File Monitoring
4. Compliance Tracking

Depending on the feature, EventSentry either

- collects information in the database
- logs alerts to the event log
- both

The diagram below illustrates the flow of information and alerts and how the individual monitoring components interact with each other:



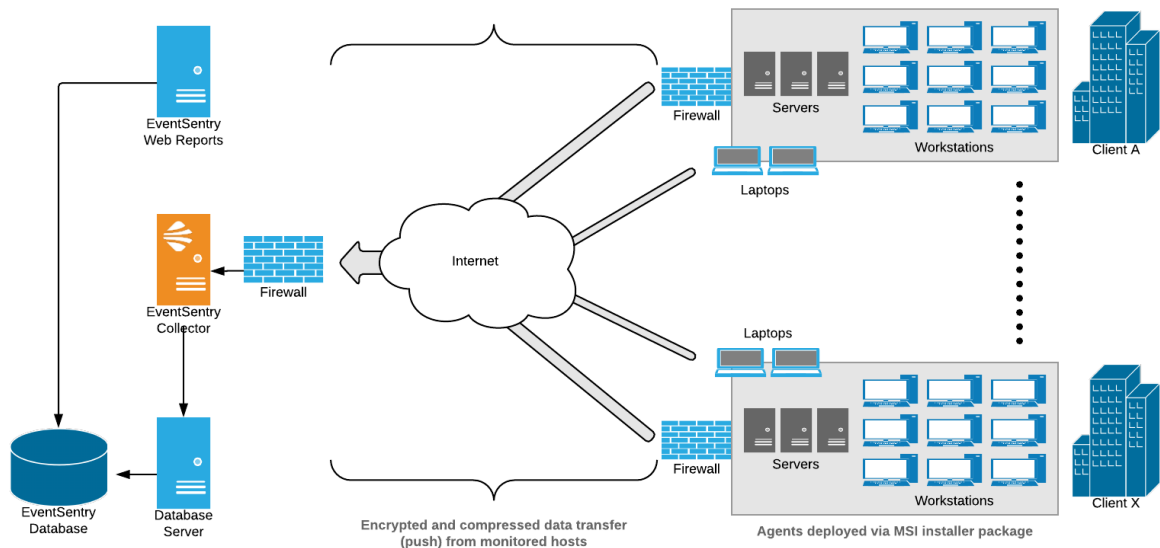
4.1 MSP Architecture

Since EventSentry supports a multi-tenant setup as well as granular access control in the web reports, it can be utilized by Managed Service Providers (MSP) to monitor their client's networks.

EventSentry can be installed and configured in multiple ways, with different levels of data isolation, to support remote monitoring. The diagrams below illustrate the different supported scenarios.

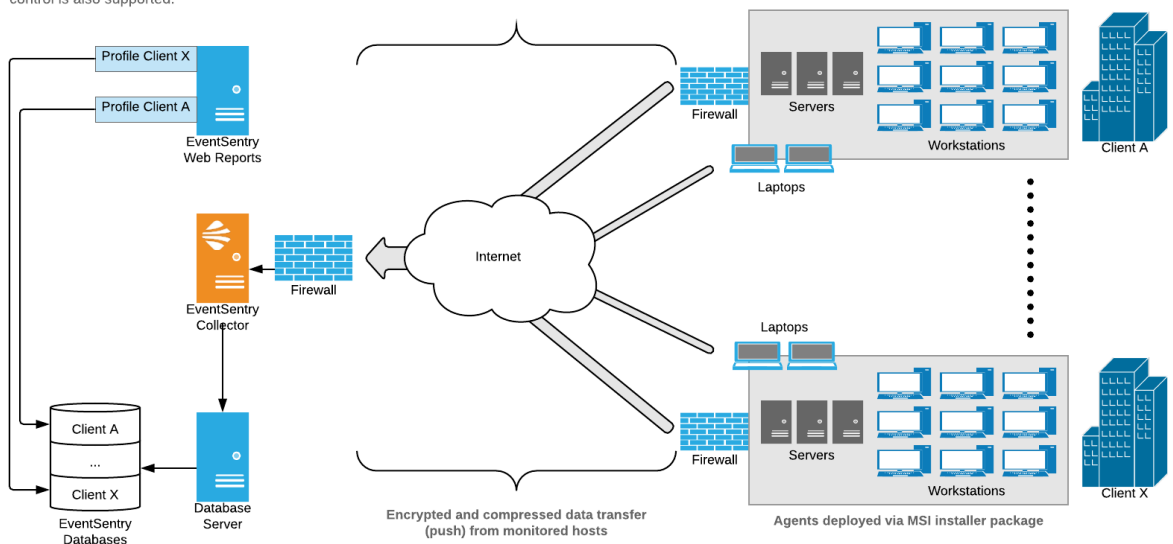
A: Managed EventSentry Installation with a Single Database

In this scenario, each client is managed as a group in EventSentry, and all collected data is stored in a single EventSentry database and accessed via the web reports. Granular access control in the web reports is supported.



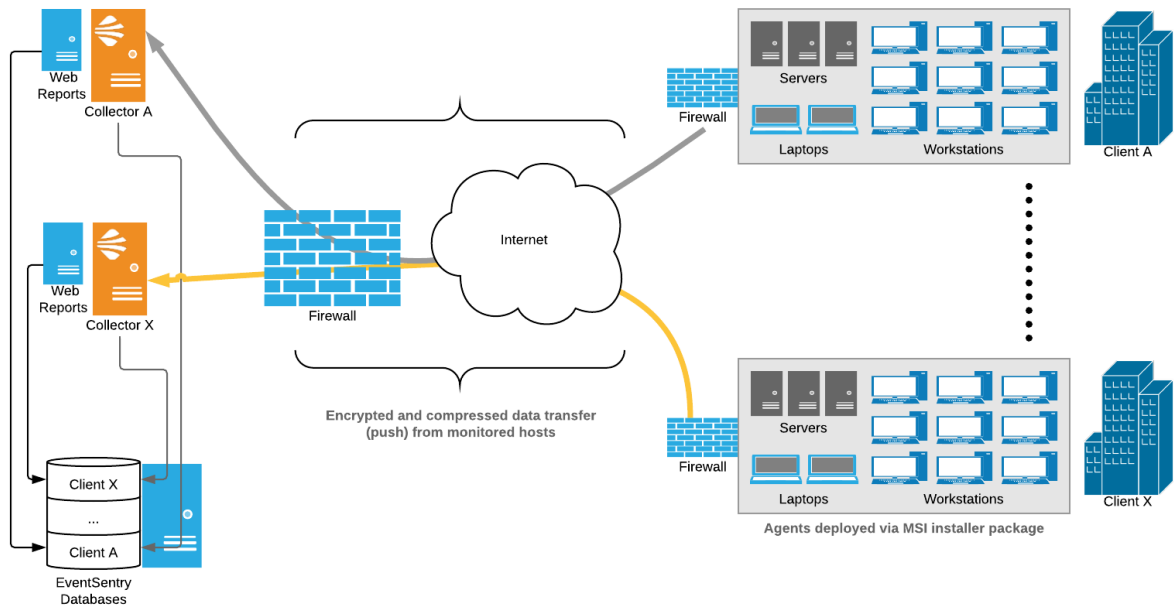
Managed EventSentry Installation with Multiple Databases

In this scenario, each client is managed as a group in EventSentry, and data from each client is stored in a separate EventSentry database for full isolation and accessed via the web reports. Multiple profiles in the web reports provide access to the various databases, granular access control is also supported.

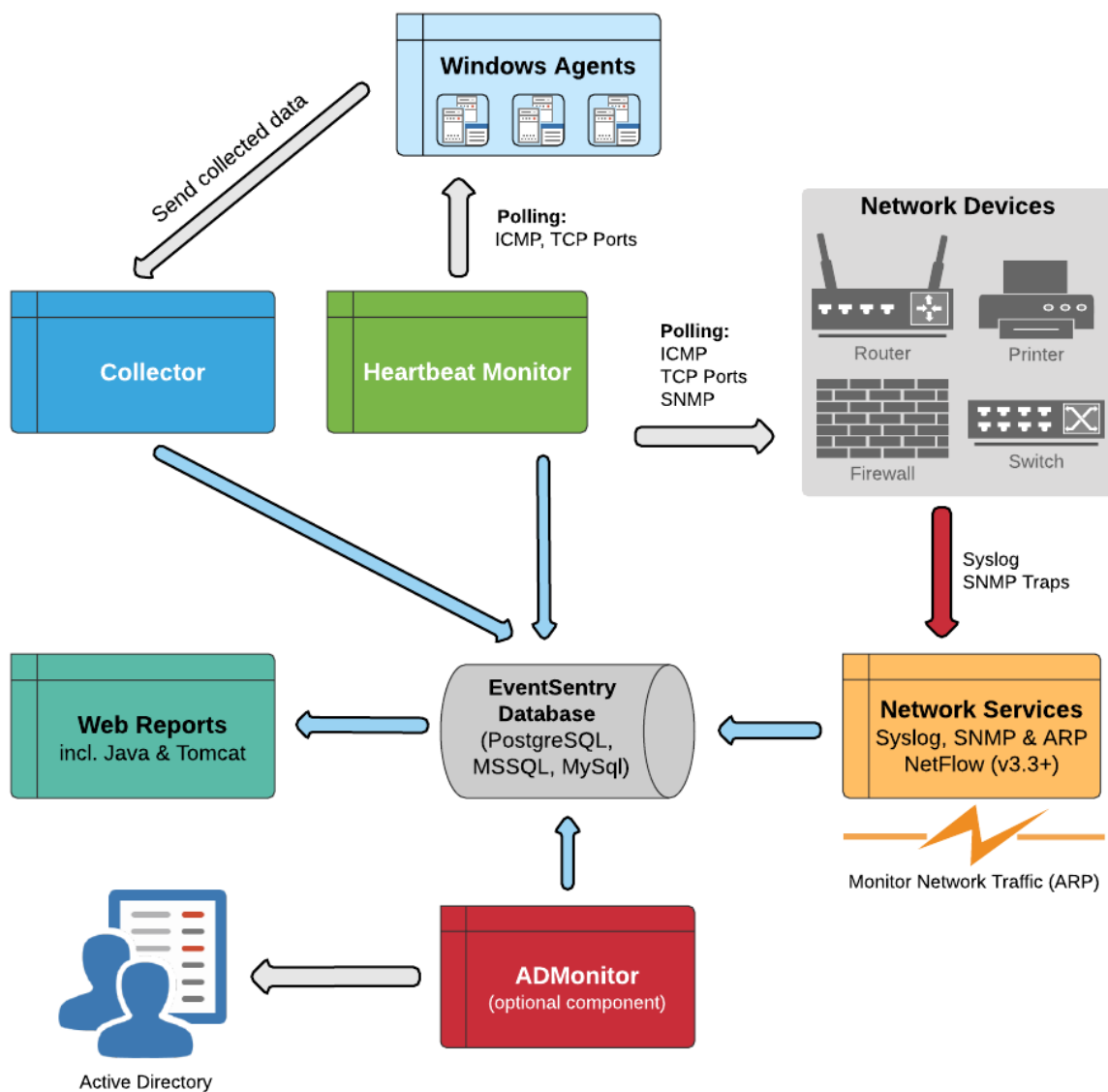


Managed EventSentry Installation with Multiple Collectors

In this scenario, each client is managed by a separate EventSentry installation, but utilizing a single central database server with multiple databases.



5 EventSentry Components



6 Heartbeat Monitoring

Heartbeat monitoring complements the agent-based monitoring of the event logs and system health. With the heartbeat monitoring feature you can monitor remote hosts from one central location.

Heartbeat monitoring supports the following monitoring features:

1. Ping

Monitor remote hosts using ICMP packets. This feature is highly customizable as you can define the number and size of packets sent, and how many percent you expect to go through.

2. TCP

Verify that applications that are listening on TCP ports (e.g. web server, email server) are active by checking one or more TCP ports.

3. EventSentry Agent

The heartbeat agent can monitor the status of the EventSentry event log and system monitoring agent to make sure that it is active and running.

4. SNMP Monitoring

Non-Windows machines (e.g. switches, routers, Unix-based hosts) can be monitored via SNMP to retrieve SNMP counters (performance, disk space) and system information.

Heartbeat monitoring offers the following reports and alerting methods:

1. Web Reports through EventSentry Web Reports

The heartbeat agent can write the current status of hosts and record a history of status changes in a database. You can then view real-time reports through the same web reports you are already using for event log and system health.

2. Local HTML status pages

If you do not have a web server and/or database available, the heartbeat agent will create HTML pages that you can either view through the management console or with a web browser.

3. Alerting through any supported EventSentry alerting method

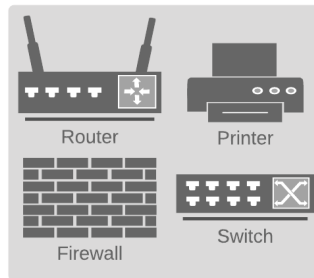
In addition to the real-time reports you can be alerted of critical status changes by any of the notification changes supported by the EventSentry agent (email, Syslog, SNMP, etc.). For example, you can receive an email when a host goes offline and/or back online. Please note that the EventSentry agent will need to be installed in addition to the heartbeat agent for this to work.



Non-Windows Servers monitored
via Ping, TCP & SNMP

Ping			Agent			TCP		
	OK			OK			OK	
	Warning			Warning			Warning	
	Error			Error			Error	

Date / Time	Computer	IP Address	Status	Ping	Agent	TCP	Ports Monitored	Ping Roundtrip	Uptime	Downtime	Availability	Last S
Thu 2016-02-25 12:52:10 PM		10.100.1.1	OK	OK	n/a	n/a		0ms	8y 133d 9h 35m 16s	2d 9h 5m 15s	99.91 %	0s
Thu 2016-02-25 12:52:10 PM		10.100.1.2	OK	OK	n/a	n/a		0ms	8y 133d 10h 4m 53s	5d 6h 42m 13s	99.78 %	0s
Thu 2016-02-25 12:52:10 PM		10.100.1.3	OK	OK	n/a	n/a		0ms	1y 133d 6h 15m 21s	17h 2m 37s	99.87 %	0s
Thu 2016-02-25 12:52:10 PM		10.100.1.4	OK	OK	n/a	n/a		0ms	1y 133d 6h 51m 27s	16h 25m 31s	99.65 %	0s
Thu 2016-02-25 12:52:10 PM		10.100.1.5	OK	OK	n/a	n/a		0ms	1y 133d 5h 51m 16s	17h 25m 44s	99.87 %	0s
Thu 2016-02-25 12:52:10 PM		10.100.1.6	OK	OK	n/a	n/a		0ms	1y 133d 6h 50m 15s	16h 18m 40s	99.65 %	0s
Thu 2016-02-25 12:52:10 PM		10.100.1.7	OK	OK	n/a	n/a		0ms	1y 133d 7h 15m 16s	15h 55m 52s	99.85 %	0s
Thu 2016-02-25 12:52:10 PM		172.16.1.1	OK	OK	OK	n/a		1ms	8y 22d 10h 1m 57s	16h 18m 36s	99.96 %	1s
Thu 2016-02-25 12:52:10 PM		192.168.1.1	OK	OK	OK	n/a		15ms	1y 93d 9h 46m 18s	4h 38m 5s	99.96 %	3s
Thu 2016-02-25 12:52:10 PM		172.16.1.2	OK	OK	OK	n/a		0ms	4y 311d 18h 42m 24s	5d 8h 17m 30s	99.81 %	1s



Network Devices

11050

EventSentry

Application

Error (Info)

Heartbeat Monitoring

11/26/2015 12:31:14 PM

2940503

The PING status of host T501 (Servers) remains at ERROR due to error "100% packets lost".

Forwards all heartbeat alerts to a customized heartbeat email action



Windows Servers and Workstations



EventSentry
Heartbeat Monitor

7 Event Log Consolidation

You can consolidate events from multiple servers and/or workstations to a central database to

- Create a backup of one or more event logs
- Be able to search through multiple event logs network-wide and create reports
- Help become compliant with a variety of regulations, such as Sarbanes-Oxley, PCI, HIPAA and more

In order to setup event consolidation you will need to:

1. Setup the EventSentry database (tables, permissions, indexes) on a supported database
2. Setup the web reports on a supported web server (IIS or Apache)
3. Create database action in EventSentry that points to the database
4. Create one or more filters that reference the database action

Figure 8 illustrates an event log consolidation in a heterogenous network:

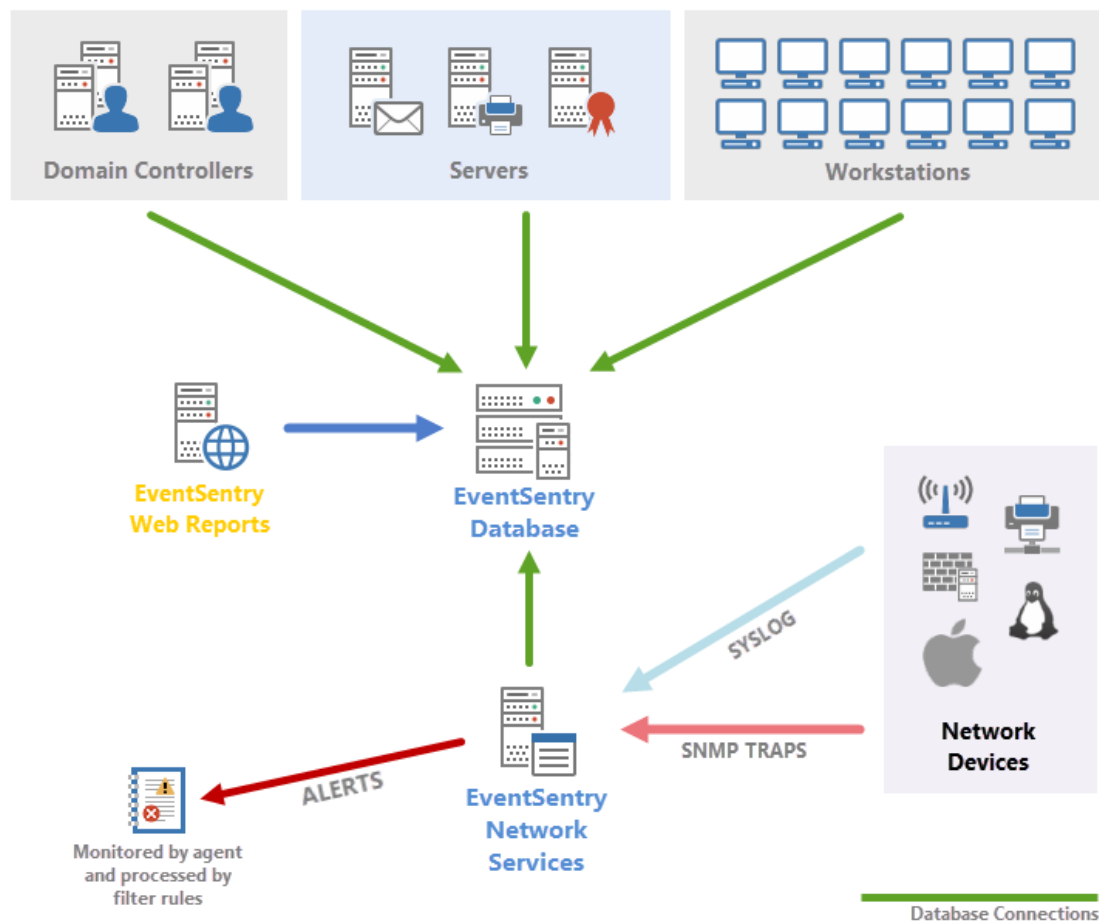


Figure 8

Syslog Message Flow

Using the Syslog feature you can also store events generated on non-Windows device in the database. Unix based machines (here Linux and OpenBSD machines) and many network devices send Syslog messages over the Syslog UDP/TCP protocol to a Windows machine running EventSentry with the Syslog daemon running. This host in turn forwards all Syslog messages, according to your filter rules, to one or more actions.

Starting with version 2.80, the Syslog daemon can also consolidate incoming Syslog messages directly into the EventSentry database, without the need of going through the Application event log. This is useful when you do not need to receive Syslog alerts and/or if you need to consolidate large amounts of data.

1. A Syslog message is sent by a device which supports the Syslog protocol
2. The Syslog message is received by the EventSentry Syslog daemon
3. The Syslog message is written to the **Application Event Log** on that machine
4. EventSentry, monitoring the **Application** event log, forwards the event record with the Syslog message



Syslog messages are first written to the application event log where they are then picked up by EventSentry and forwarded to the configured action, according to the configured filters.

8 More Information

For more information on EventSentry please read the help file **eventsentry_hlp.chm** which is included in the installation package. Alternatively you can access all EventSentry help material from <http://www.eventsentry.com/support/kb>.

If you cannot find answers to your questions in the provided help materials then please send an email to support@netikus.net. Registered customers will receive immediate attention, EventSentry Light users please post any questions in our forums at <http://forums.netikus.net>. Thank you.