

---

# EventSentry Overview

<b>Part I About This Guide</b>	<b>1</b>
<b>Part II Overview</b>	<b>2</b>
<b>Part III Installation &amp; Deployment</b>	<b>4</b>
1 Installation with Setup .....	5
2 Management Console .....	6
3 Configuration .....	7
4 Remote Update .....	10
<b>Part IV Monitoring Architecture</b>	<b>13</b>
<b>Part V Heartbeat Monitoring</b>	<b>14</b>
<b>Part VI Event Log Consolidation</b>	<b>16</b>
<b>Part VII More Information</b>	<b>19</b>

## 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/support\\_help.php](http://www.eventsentry.com/support_help.php).

This overview covers the following topics:

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

## 2 Overview

EventSentry is a Windows monitoring suite to monitor the event logs, system health and uptime of any Windows 2000 or higher computer. EventSentry consists of four main parts:

- Management Console
- Windows Agent
- Heartbeat Agent
- 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.

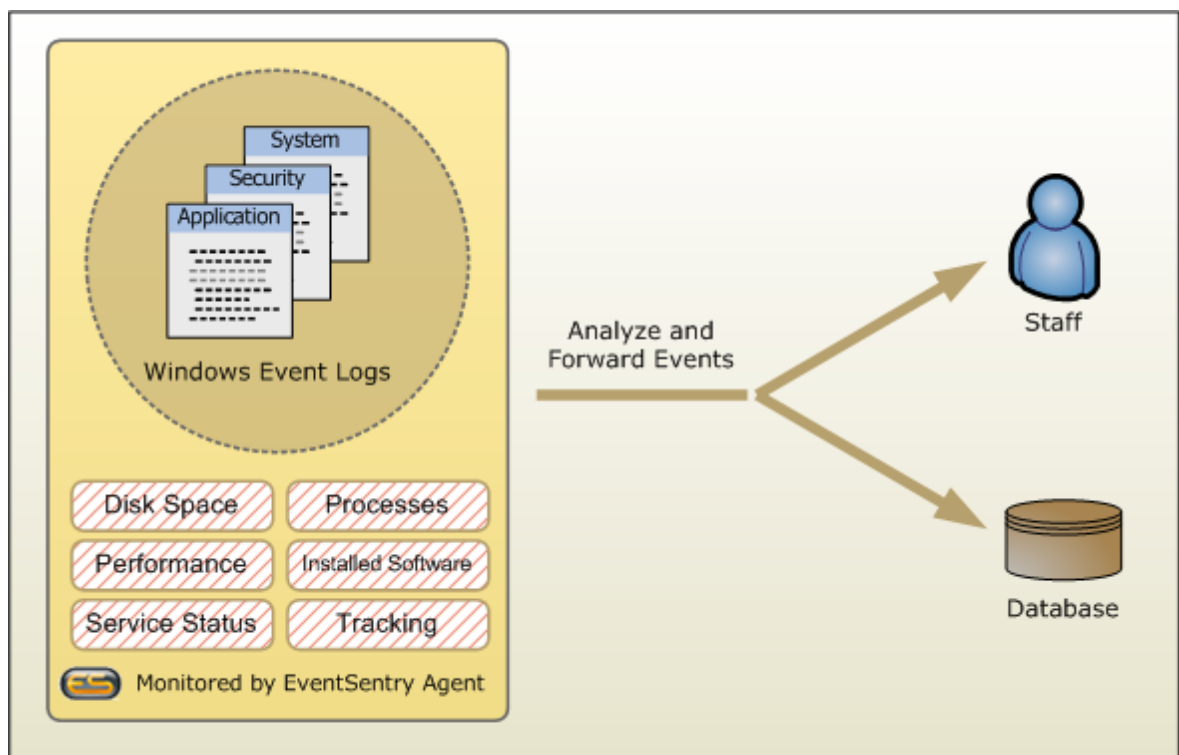


Figure 1

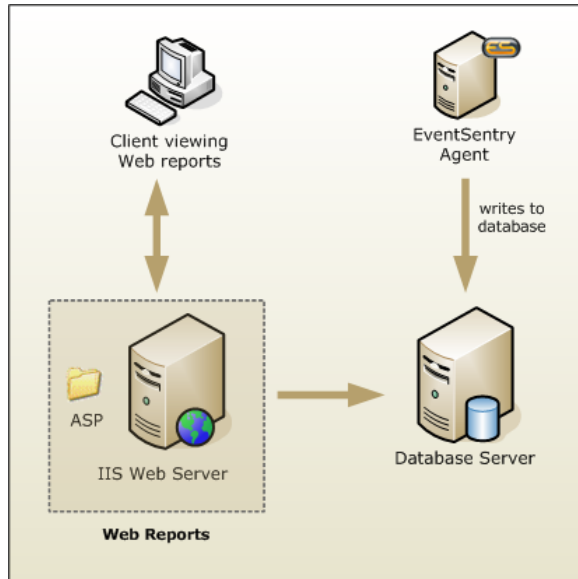


**Please note** that the agent must be installed on **every** computer that is to be monitored.

## Heartbeat Agent

The EventSentry heartbeat agent monitors the uptime of remote hosts through ping (ICMP) and TCP connections, and it can also monitor the status of the EventSentry event log agents.

## Web Reports



The web reports consist of a collection **ASP** files that are copied to an IIS web server. With the web reports you can:

- View overall **Network Health**
- Search for **Event Log** entries and create reports
- Search for text in delimited or non-delimited **log files**
- View **Compliance** reports
- View **Print Job** information
- Display **Event Log** statistics
- Display **Performance Charts** and query **Performance Data**
- View **Disk Space** trends and reports
- View **Heartbeat Status, Heartbeat History** and **Heartbeat Uptime**
- View **Service Status, Service History** and **Service Uptime**
- View **Installed Software, Installation History**
- View **System & Hardware Information**
- View **Environment Monitoring** graphs
- View reports for **Nessus** scan files

### 3 Installation & Deployment

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

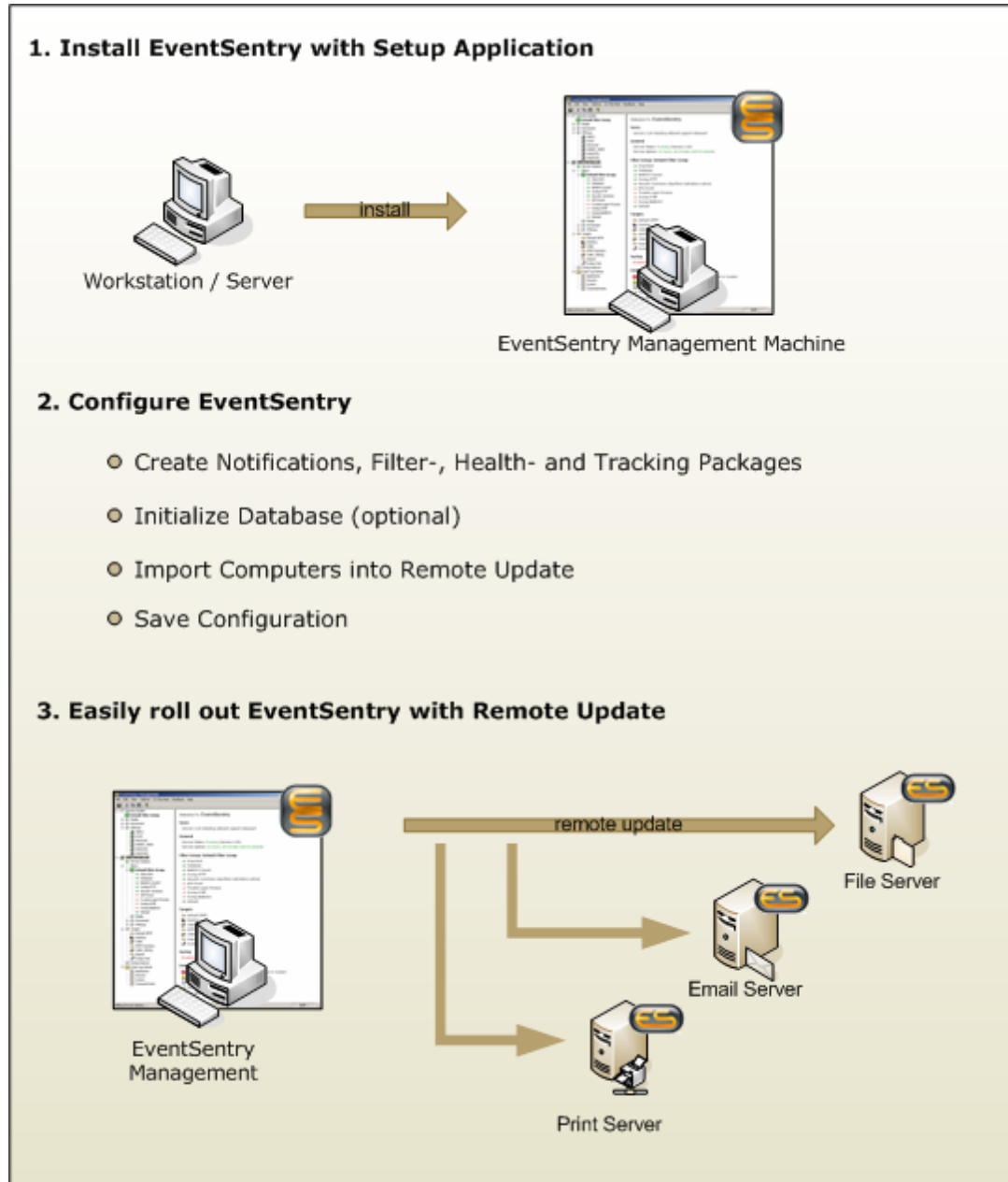


Figure 2

### 3.1 Installation with Setup

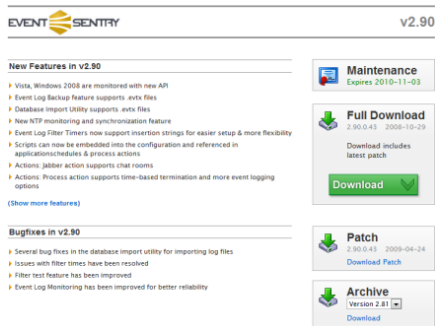


Figure 3

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

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.

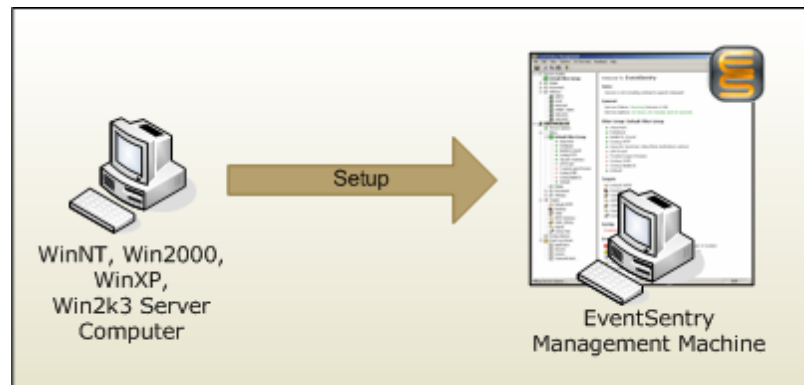
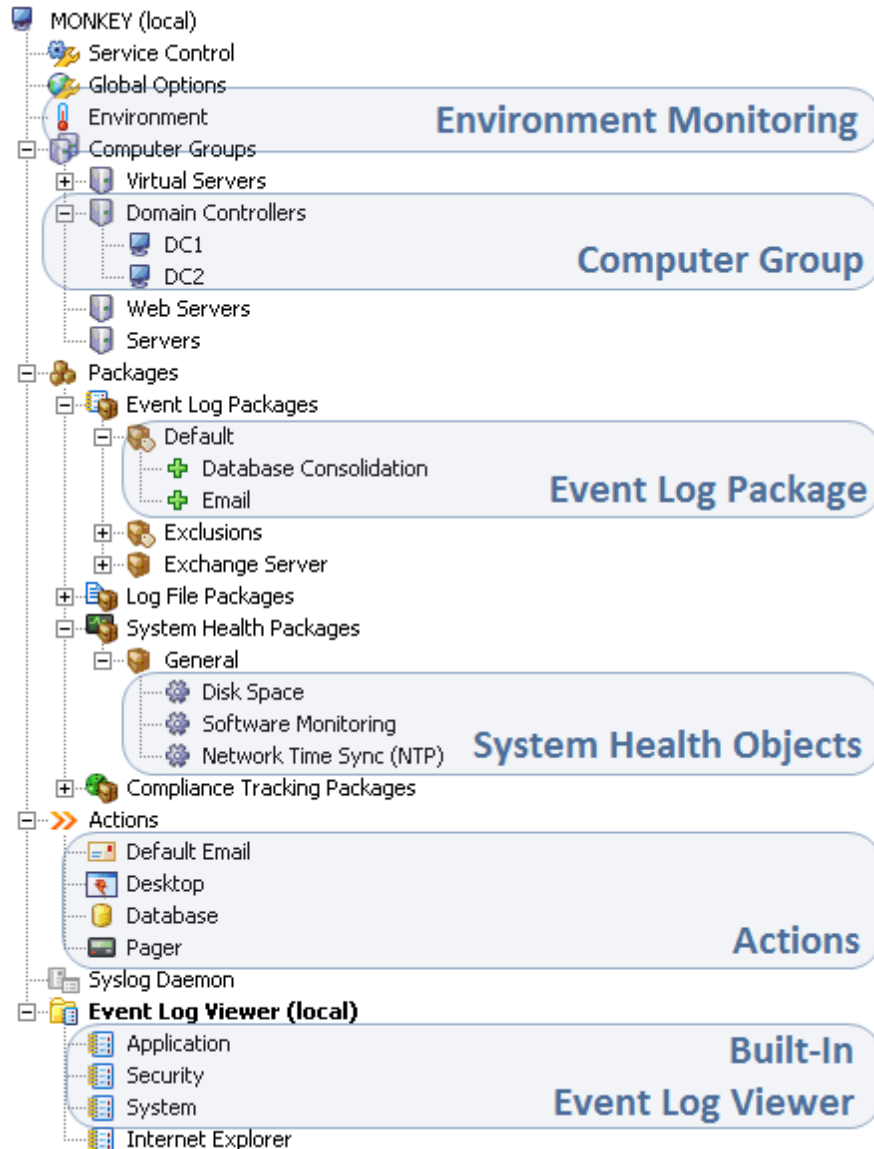


Figure 4

## 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**.

You can access most features by simply clicking on the container on the left, but many features (e.g. filters, actions) require you to right-click them in order to make changes. For example, you need to right-click an **Event Log Package** container in order to add a new filter.



## 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 filter, health and tracking packages
- One action (*Default SMTP*)

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):

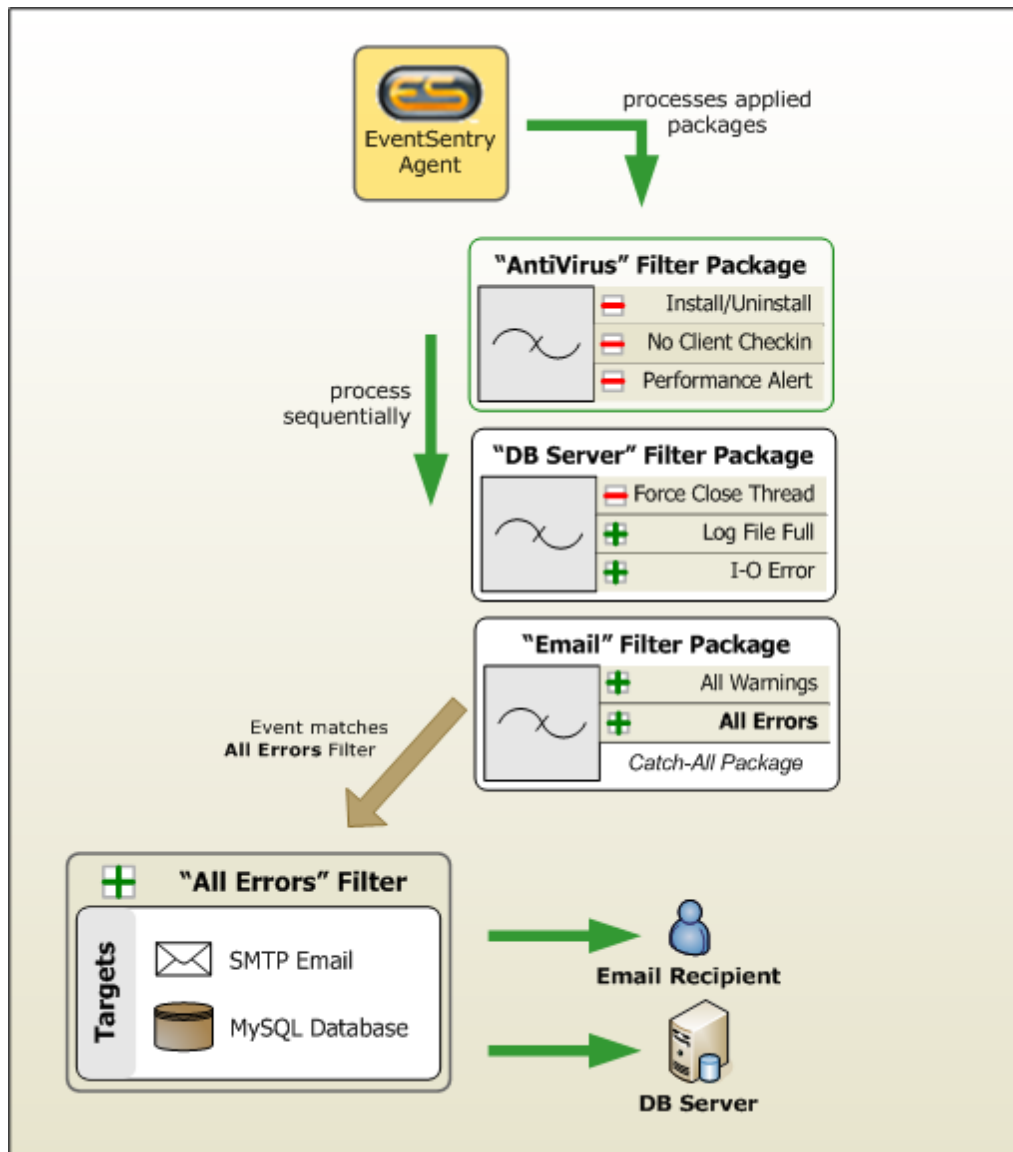


Figure 5

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 **All Errors** filter and is forward to both configured notifications (SMTP Email & MySQL Database).

### 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\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.

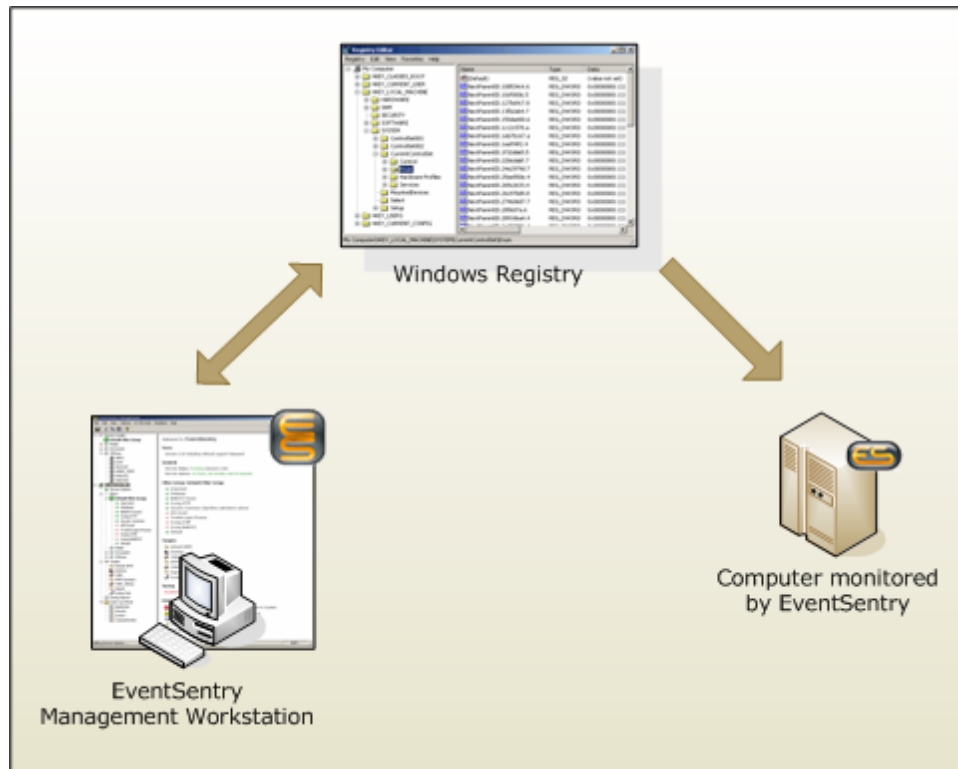


Figure 6

## 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. **Install & Configure 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. With "Update Configuration" you can push the entire configuration to the remote computer.
3. **Manage Agent(s) -> Update:** 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. Make sure that you configure the new options first, before you roll out the new agents.

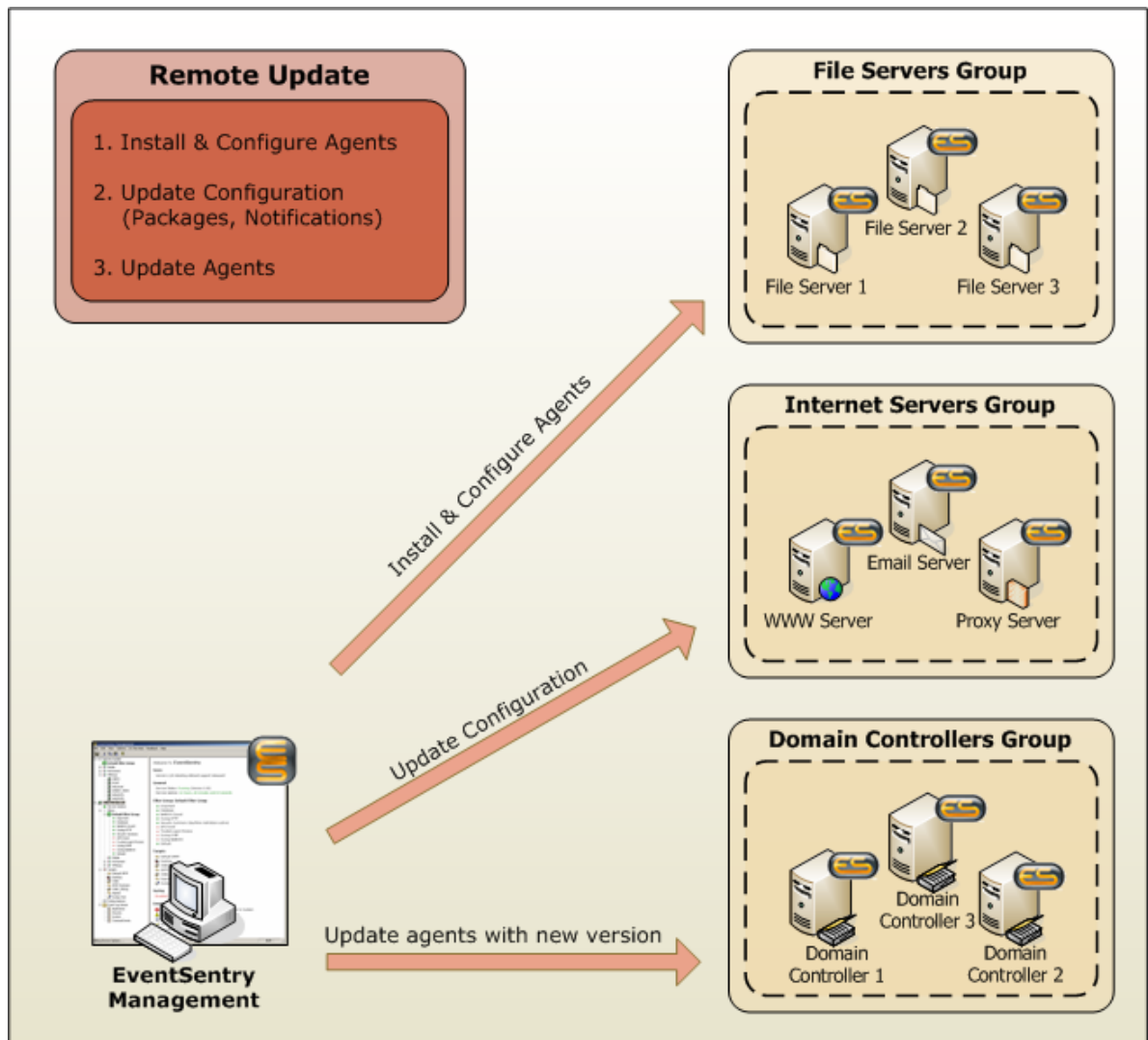


Figure 7

### 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 **Install & Configure 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 **Update 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

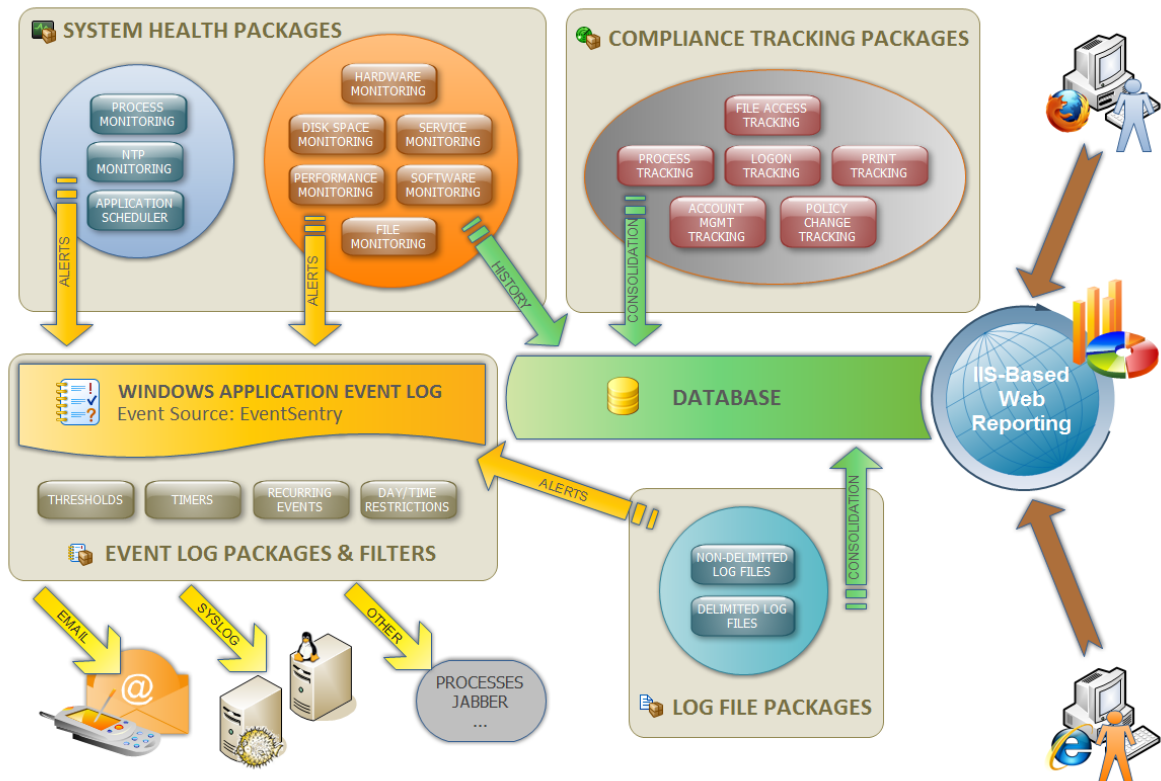
The diagram below shows how the individual components inside the EventSentry agent either alert and/or collect information in the database. The agent includes the following 4 major monitoring components:

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

Please see the diagram below for more information on the individual monitoring components.



## 5 Heartbeat Monitoring

Heartbeat monitoring is the ideal complement to 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.

Heartbeat monitoring offers the following reports and alerting methods:

#### 1. Web Reports through EventSentry Web Reports

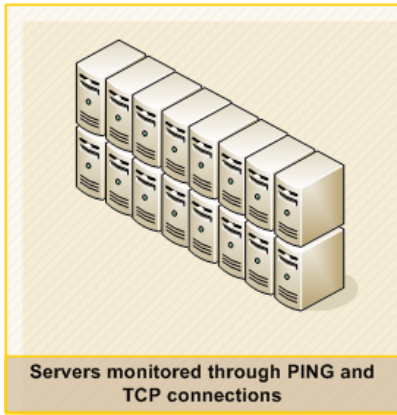
The heartbeat agent can write the current status of hosts and record a history of status changes in a database. You can then view real-time reports through the same web reports you are already using for event log and system health.

#### 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.

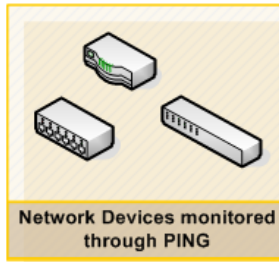
#### 3. Alerting through any supported EventSentry alerting method

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.



1. View Heartbeat Status through Web Reports

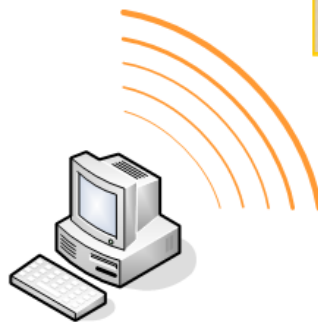
Computer	Status	Ping	Agent	TCP	Ports Monitored	Ports Failed	Ping Roundtrip	Information	Last Check
FIREWALL	OK	OK	n/a	n/a			0 ms		2/6/2006 11:00:23 AM by VMALE
JAGUAR	OK	OK	n/a	n/a			0 ms		2/6/2006 11:00:23 AM by VMALE
JURKBOX	OK	OK	n/a	OK	22		0 ms		2/6/2006 11:00:23 AM by VMALE
MAL.AMATACORP.COM	OK	OK	n/a	OK	25		143 ms		2/6/2006 11:00:23 AM by VMALE
WWW.NETIKUS.NET	OK	OK	n/a	OK	22 25 80		207 ms		2/6/2006 11:00:23 AM by VMALE
BELUGA	OK	OK	OK	OK	21 3306 22		0 ms		2/6/2006 11:00:24 AM by VMALE
KANGAROO	OK	OK	OK	n/a			0 ms		2/6/2006 11:00:24 AM by VMALE
RHINO	OK	OK	OK	OK	1433		0 ms		2/6/2006 11:00:24 AM by VMALE
VMALE	OK	OK	OK	OK	25 53 80 143 1433		0 ms		2/6/2006 11:00:24 AM by VMALE



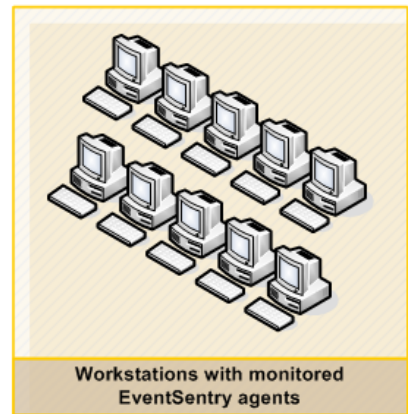
2. Immediate Notification through EventSentry

```

EVENT #      4729
EVENT LOG    Application
EVENT TYPE   Error
SOURCE      EventSentry
CATEGORY    HeartBeat Monitoring
EVENT ID     11000
COMPUTERNAME RACON
TIME        1/16/2005 10:27:19 PM
MESSAGE     Host WWW.MICROSOFT.COM (Internet Hosts) changed its Ping
            status from OK to ERROR. The reason for the status change
            was: "100% packets lost".
    
```



**EventSentry Management Workstation with Heartbeat Monitor**



## 6 Event Log Consolidation

You can consolidate events from multiple servers and/or workstations to a central ODBC 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 government regulations, such as Sarbanes-Oxley, 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 a ODBC Target notification in EventSentry that points to the database
4. Create one or more filters that reference the ODBC Target

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

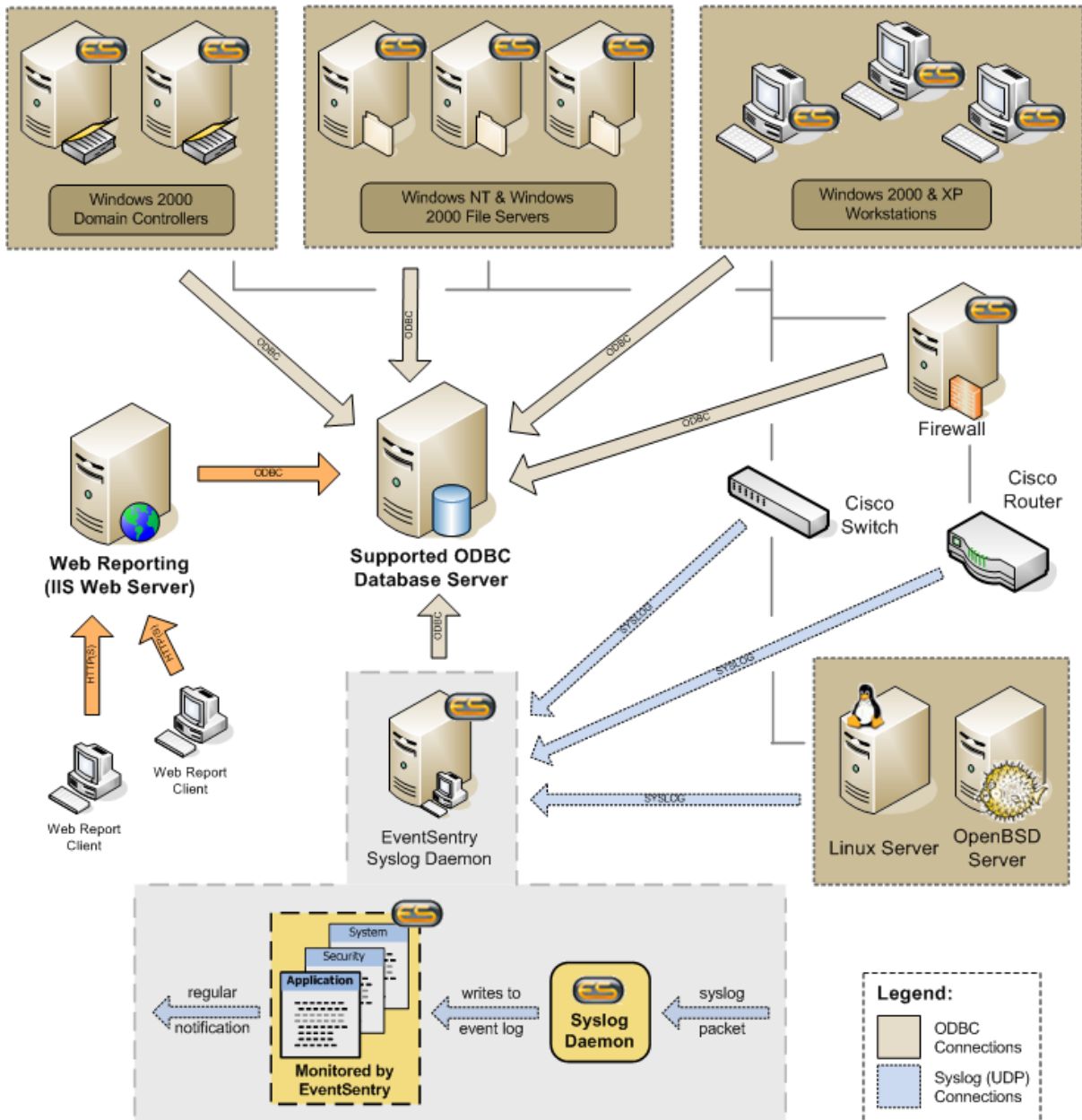


Figure 8

### 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



As you can see, 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.

## 7 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\\_help.php](http://www.eventsentry.com/support_help.php).

If you cannot find answers to your questions in the provided help materials then please send an email to [support@netikus.net](mailto: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.