IPSWITCH

WhatsUp Event Archiver v10.x Importer Guide

Using the WhatsUp Event Archiver Importer

How Event Archiver Importer Works 2
System Requirements 3
Integrating With Event Archiver 4
Configuring Event Archiver Importer 5

Using the WhatsUp Event Archiver Importer

In This Guide

How Event Archiver Importer Works....2
System Requirements....3
Integrating With Event Archiver....4
Configuring Event Archiver Importer....5

How Event Archiver Importer Works

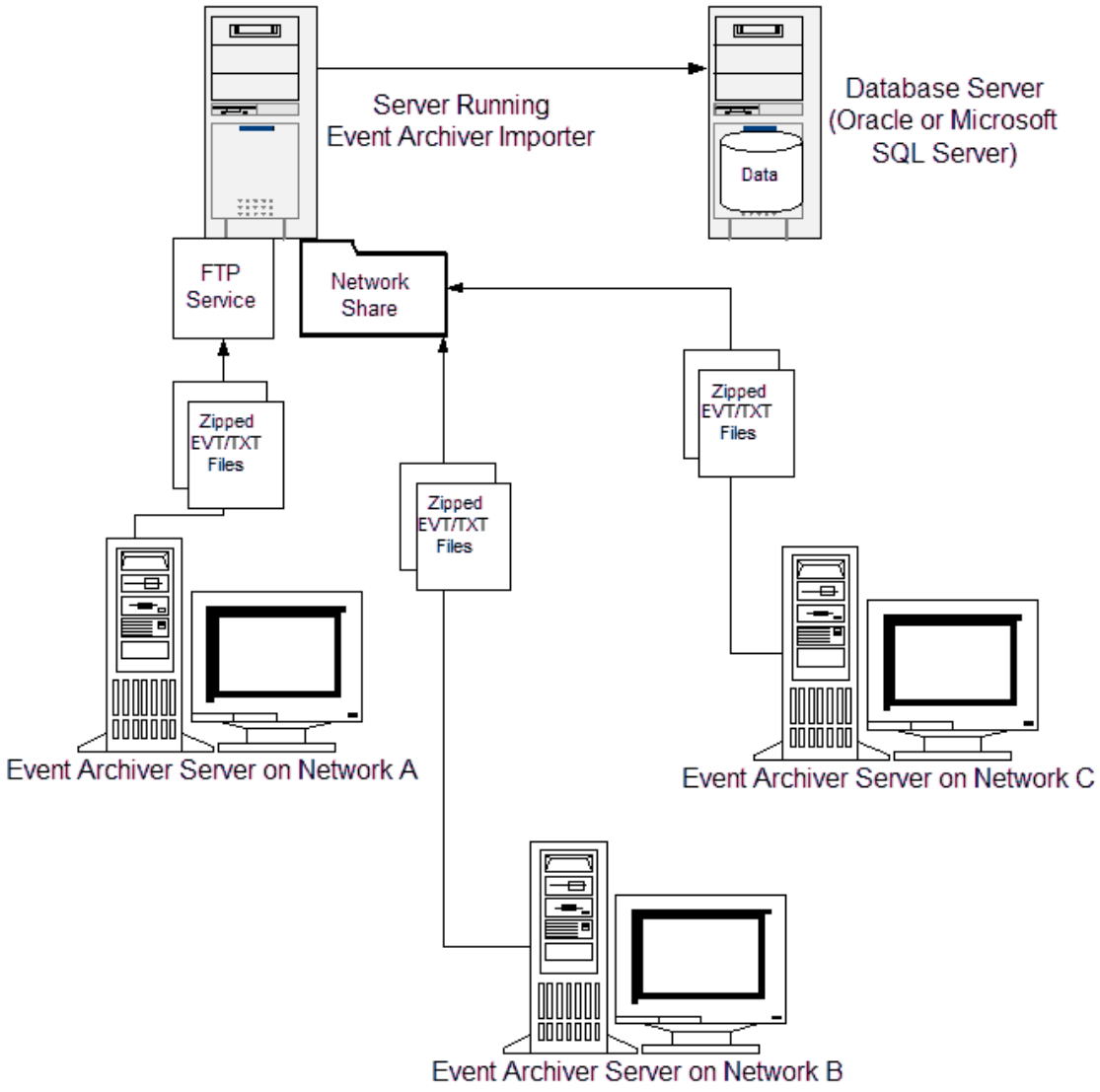
The Event Archiver Importer utility is designed to load event log data collected from Event Archiver installations on different or bandwidth-limited networks into one central database server.

For example, some users of Event Archiver may have branch offices connected by WAN links, with limited network bandwidth to transfer uncompressed log data directly to a central database server during collection. Other users may have multiple untrusting domains running within a single physical network, yet must consolidate all log data from all domains into a central database server. The Event Archiver Importer utility provides a solution for these and other challenging scenarios.

To accomplish these tasks, the Event Archiver Importer utility constantly polls a directory on the computer where it is installed for incoming compressed log files collected by various Event Archiver installations throughout the network. Each Event Archiver installation can be configured to transmit these compressed log files automatically via standard Windows Network shared folders OR via FTP. After the files arrive in the incoming directory, the Event Archiver Importer Service immediately decompresses them and imports their contents into centralized tables on an Oracle or Microsoft SQL database server.

Only comma-delimited text files (uncompressed or compressed) are actually read into the database. Compressed or uncompressed EVT/EVTX files are stored in a final destination of the administrators' choosing.

Review the following diagram below to see how the Event Archiver Importer utility works in conjunction with various Event Archiver installations and a central database server.



System Requirements

The system resources used most by the Event Archiver Importer utility are CPU cycles and memory. File storage requirements can be minimized by using a UNC Path as the Final Storage directory. Below are the minimum requirements needed for the computer where the Event Archiver Importer is installed.

CPU. A Pentium-III class CPU running at 1Mhz or greater.

RAM. 256 MBs of memory minimum; 512 MBs are recommended.

Disk Space. 500 MBs of free disk space for temporary decompression of compressed files; 5-10 GBs of free disk space if the computer running the Event Archiver Importer utility is permanently storing the saved flat files.

Integrating With Event Archiver

To Integrate the Event Archiver Importer with Event Archiver:

1. Install the Event Archiver Importer setup package on a computer receiving the incoming compressed EVT/EVTX and comma-delimited text files from Event Archiver installations throughout your network.
2. Configure the Event Archiver Importer Service's operating properties, including its resource limits, database table links, file directories, and service account.
3. In the Event Archiver Importer installation directory, share the Incoming subfolder on the network if Event Archiver installations forward log files via Windows File Sharing. If Event Archiver installations forward log files via FTP, no sharing is needed, but you need to make the Incoming directory the root directory or a virtual folder in your FTP server software.

   Ensure the account used as the Event Archiver Service account throughout your domain has FULL CONTROL access to this share point. Also, ensure that all domain administrators have FULL CONTROL to this share access point. This is important in case a domain administrator occasionally initiates archiving manually on certain Event Archiver systems using their interactive account. Failure to set appropriate access rights can result in File/Path errors on various Event Archiver installations trying to send their logs to the Incoming share. No less than FULL CONTROL access to the share and underlying NTFS directory suffice for both the Domain Admins group, as well as the Event Archiver Service domain account.

   If Event Archiver uses FTP to forward log files to the Incoming directory, ensure that the FTP account various Event Archiver installations use has at least CREATE, WRITE, and MODIFY permissions in the Incoming directory.
4. Point Event Archiver installations forwarding zipped text files and EVT/EVTX files to the shared folder you created in Step 2, or to the computer running the FTP Server and Event Archiver Importer software if you are using FTP.

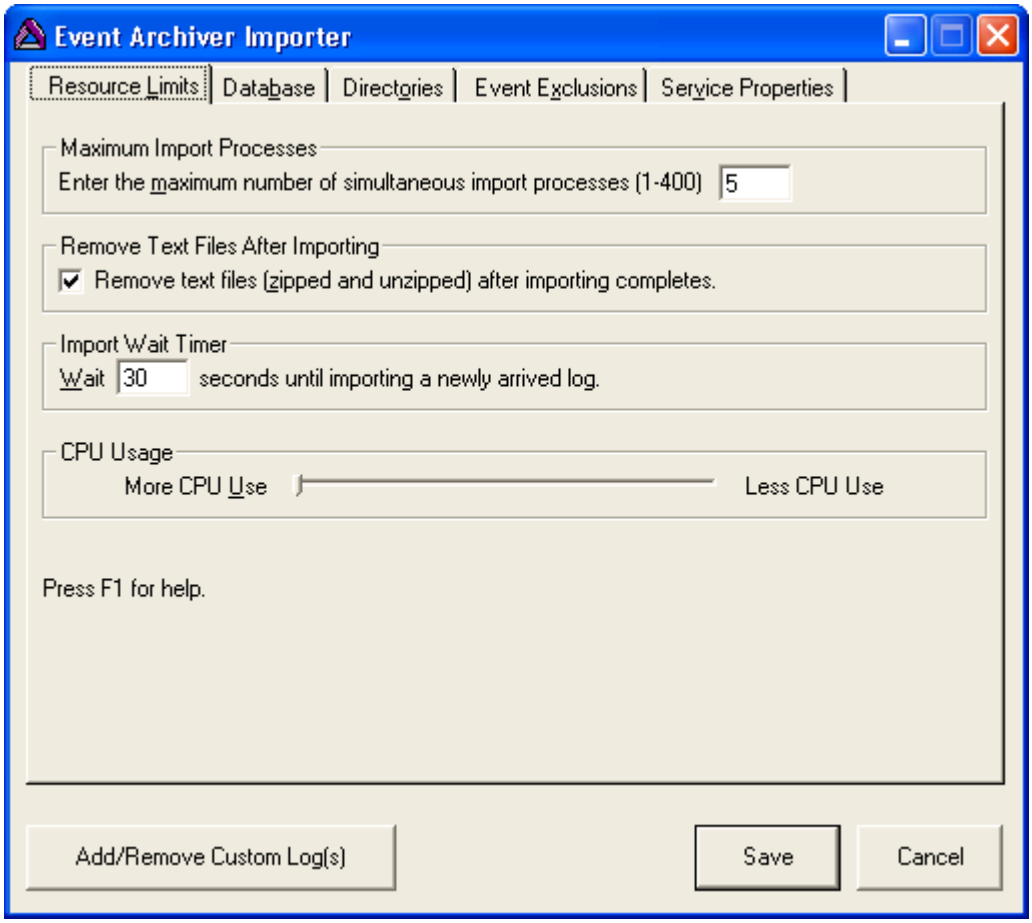
Note: Only comma-delimited text files (compressed and uncompressed) are read into the Microsoft SQL Server tables. EVT/EVTX Files (compressed and uncompressed) are sent immediately to the final destination directory.

5. Verify that you have created the appropriate database tables (one per each log type) in your Microsoft SQL Server or Oracle database. You can do this manually by using the Create Microsoft SQL Server Table(s) or Create Oracle Database Table(s) tools located under the **Tools > Database Helpers** menu in the Event Archiver program. If the tables are not created, create the following tables in your database using the tools mentioned above:
   - Application
   - System
   - Security

- DNS Server
- Directory Service
- File Replication Service

Configuring Event Archiver Importer

Resource Limits Tab



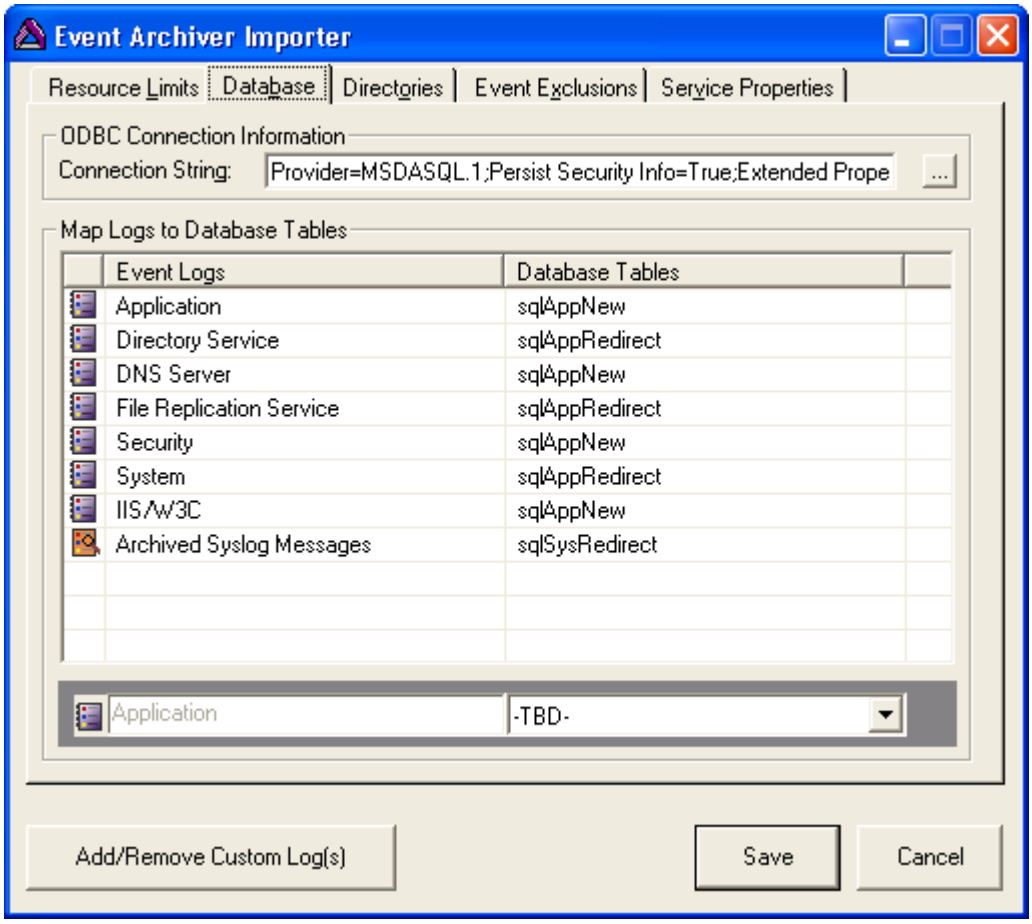
- **Maximum Import Processes**. Controls how many simultaneous helper processes can be launched by the service to import text files into the ODBC database. Enter a number between 1 and 400. The default is 5.

Note: Each additional process, while running, can use approximately 5MBs of memory. However, not all processes run concurrently unless there are many files in the Incoming directory.

- **Remove Text Files After Importing**. Controls whether the Event Archiver Importer Service deletes comma-delimited text files after they are successfully read into the database. Check the option if you would like the comma-delimited text files deleted after the import completes.

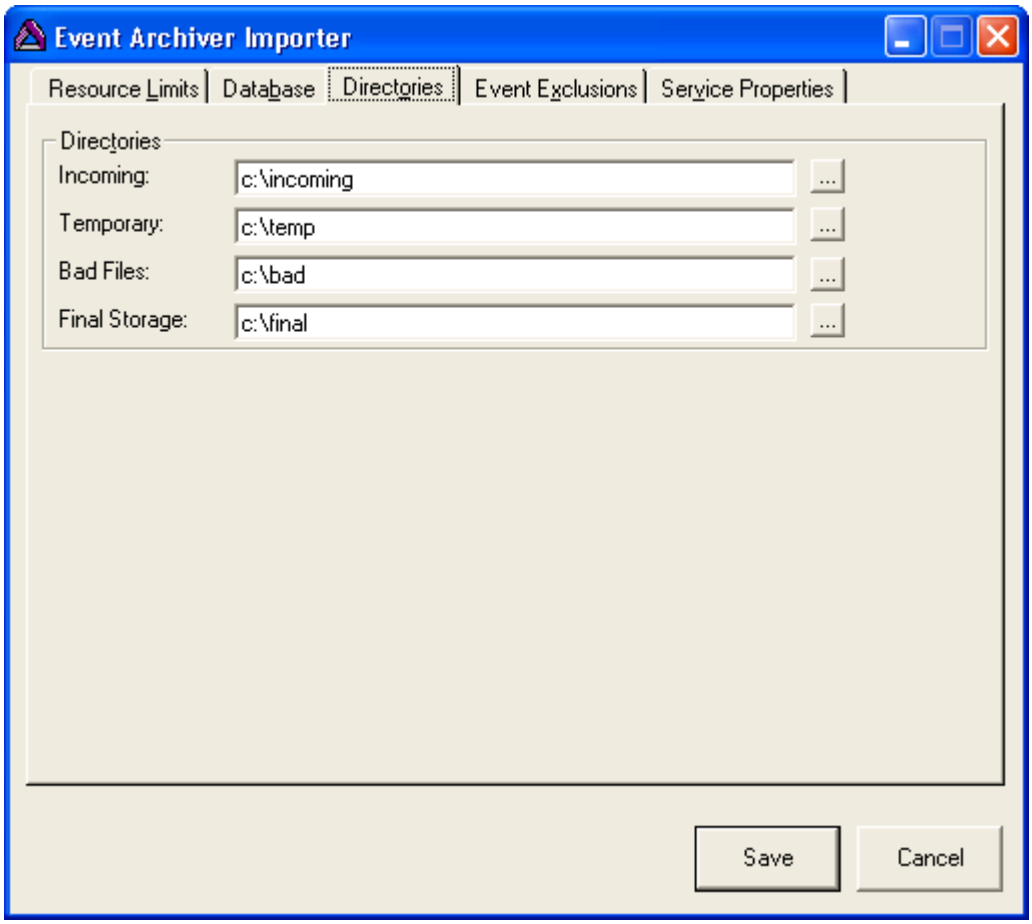
- **Import Wait Timer**. Controls how long the Event Archiver Importer Service waits after detecting that a log file is completely transferred into the incoming network share. The default is 30 seconds. If you have file contention issues, consider increasing this value.
- **CPU Usage**. Move the slider to the right to increase the amount of rest cycles the Event Archiver Importer Service takes importing a log file, resulting in lower overall CPU use. Conversely, move the slider to the left to decreases the amount of rest cycles the Event Archiver Importer Service takes importing a log file, resulting in higher overall CPU use.

Database Tab



- **ODBC Connection Information**. Click the (**...**) button to browse and select an ODBC File DSN linked to your Event Logs database in Microsoft SQL Server or Oracle. If you do not know how to make an ODBC File DSN connection, consult the Event Archiver User Guide located at the Ipswitch support site.
- **Map Logs to Database Tables**. After a valid ODBC connection is established, the Database Table list populates with available tables from your Event Logs database on the database server. Select the appropriate table for each log type.

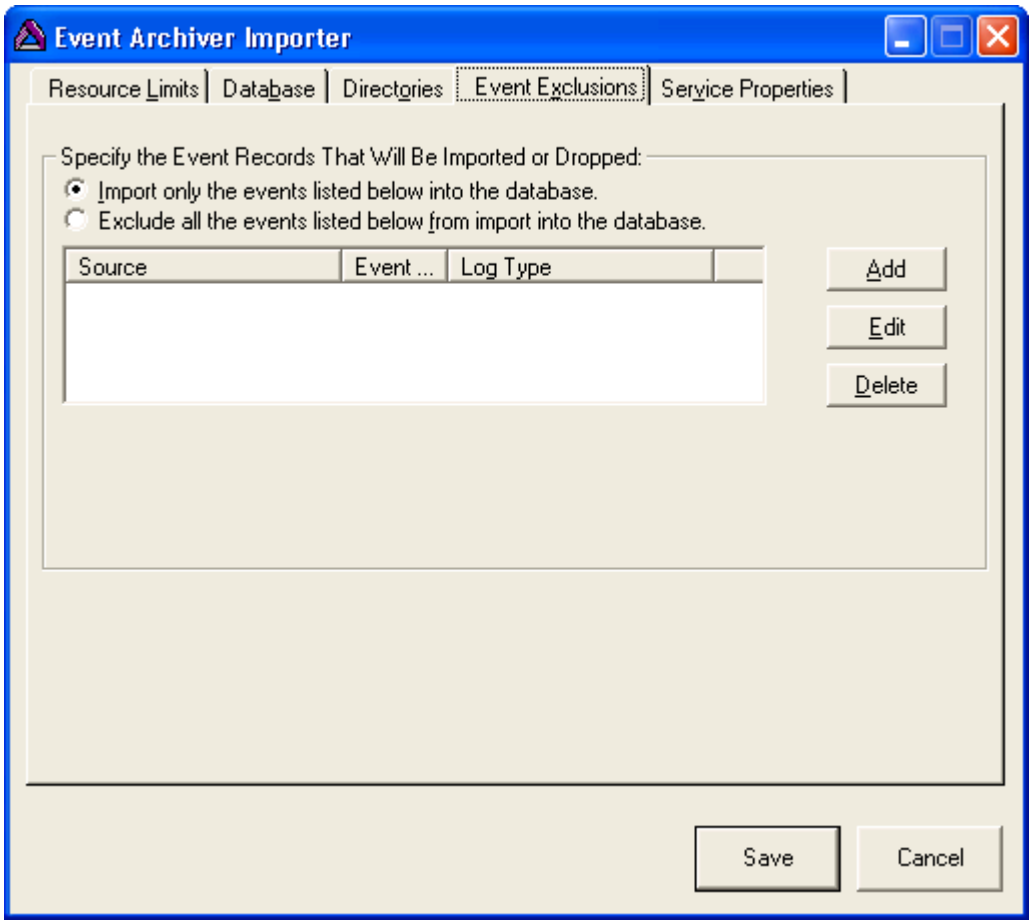
Directories Tab



- **Incoming Directory**. The directory the Event Archiver Importer Service polls continuously for incoming, zipped text and/or EVT/EVTX files. This directory must be shared on the network, or correspond to a top level directory on a FTP server.
- **Temporary Directory**. Used by the Event Archiver Importer Service when it imports log records from comma-delimited text files into database tables.
- **Bad Files**. Any files that cannot be processed by the Event Archiver Importer Service are placed here. An administrator should review and scrub this directory at regular intervals.
- **Final Storage**. Contains all files processed successfully by the service, in their native, compressed format (e.g. .zip).

Note: If you elect to use a UNC Path to move the files to a different file server for long term storage, Ensure the Event Archiver Importer Service account has adequate rights to move these files to that UNC Path.

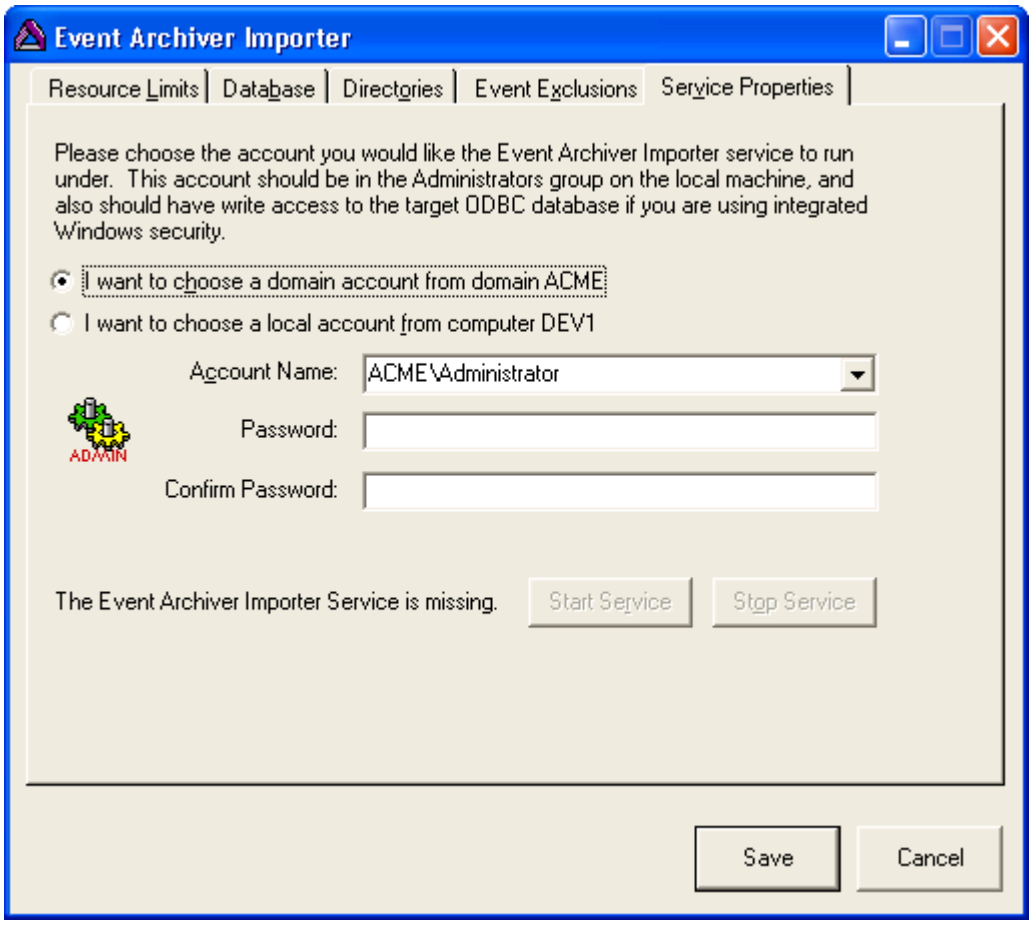
Event Exclusions Tab



From the Event Exclusions tab you can program the Event Archiver Importer service to drop certain types of events, OR only import specific events, by specifying a source name, Event ID, and log type. Depending on how you configure this area, events that match the exclusion list or that do not match an inclusion list are dropped and ignored, resulting in smaller database sizes after text file imports occur.

Note: When defining an event in this area, if you specify -1 as the Event ID, the software drops or includes all events from a given source, regardless of EventID. This is useful if you do not care about entire applications, hardware devices, etc and do not need their events in the database.

Service Properties Tab



- **I want to choose an account from**. The Event Archiver Importer Service account can run as either a domain account or a local computer account. However, the account chosen here must be in the local Administrator's group on the computer where the Event Archiver Importer utility is installed. Furthermore, the Event Archiver Importer Service account cannot run under the LocalSystem context.

Note: If your ODBC Connection Information (see above) is configured to use integrated Windows security for authentication to your database, the account you choose here must have appropriate permissions to write data to the target Event Logs database and its tables.

- **Account Name**. Select the appropriate account from the list.
- **Password**. Enter the password associated with the account name.
- **Confirm Password**. Enter the password associated with the account name for verification.
- **Start Service**. If the Event Archiver Importer Service is not running, click this button to start it.
- **Stop Service**. To shutdown the Event Archiver Importer Service, click this button to stop it.