EventVault Introduction and Usage

Feature Guide

Version 6.x
ABSTRACT

The purpose of this document is to introduce EventVault Warehouse Manager, an integral part of EventTracker for Windows and describe its usage.
Table of Contents

EventVault Warehouse Manager ............................................................................................................... 3
Methods of Archiving ............................................................................................................................... 4
  Benefits of Archiving Event Logs ............................................................................................................ 4
Agent Side Archival Process ....................................................................................................................... 5
EventTracker Scheduler Service ................................................................................................................. 5
  EventTracker Scheduler Service – Collection Master Console ............................................................. 7
  EventTracker Scheduler Service – Collection Point Console ............................................................... 7
About Archival Process ............................................................................................................................... 8
  Archival Process ...................................................................................................................................... 8
Verify EventVault Integrity ......................................................................................................................... 8
  Schedule EventVault Integrity Check .................................................................................................... 9
  Purge Archives ....................................................................................................................................... 12
Back up EventVault Data ........................................................................................................................... 13
Extract and View EventVault Data .......................................................................................................... 16
  View Extracted Event Data .................................................................................................................. 17
Delete EventBoxes .................................................................................................................................... 18
Save EventVault Summary Information ................................................................................................. 18
Move Archives ........................................................................................................................................... 19
Append Archives ........................................................................................................................................ 21
EventVault Warehouse Manager

EventVault Warehouse Manager is an integral part of EventTracker for Windows and it provides the capability to archive events from the EventTracker database. EventVault provides a simple, but important mechanism to securely archive event logs for future use and more specifically for auditing purposes.

In most enterprise networks with multiple critical servers and workstations the event log data can become huge and unmanageable. This event data may not be immediately required once the initial analysis is completed. At the same time they cannot be completely discarded, as they will be required for future audits. EventVault Warehouse Manager solves this problem and also provides mechanisms to identify if any of the archived event data has been tampered with.

Archives are .mdb files that are compressed into .cab files called as ‘EventBoxes’ and are stored in the Archives folder. If EventTracker is installed in the default path then these files could be located in the ...\Program Files\Prism Microsystems\EventTracker\Archives directory. The range of events that each EventBox contains is stored into an index file in the archives folder. These EventBoxes are sorted on period and can be viewed from EventVault Manager Window.
Methods of Archiving

EventTracker provides the following two methods of archiving:

- Agent side automatic archival (in Windows native .EVT format)
- EventVault configurable archival (in encrypted format)

The Agent side archival is done automatically whenever an event log becomes full. These archive files are stored in the EventTracker Agent directory. These files can be viewed using the Windows Event Viewer.

Benefits of Archiving Event Logs

The benefits of archiving the Event log data are as follows:

- A backup of the Event data is available in 2 formats (.evt and encrypted) and can be used for forensics
- Integrity of the encrypted archived data can be verified
- Events are viewable in standard Windows .evt format
- Enhance security
- Fulfill audit requirements
- Extract and view old event data
- Automate the archival with configurable period
- Append missing archives
Agent Side Archival Process

Agent side archival is designed to archive the event logs that become full before clearing its contents to ensure that event logging is not hindered. The archived event logs will be in the native Windows .EVT format and will be located in the EventTracker Agent directory (if installed in the default path it will be ...\Program Files\Prism Microsystems\EventTracker\Agent) and will be named in the following convention - <event log name><current time in ticks>.evt.

Sample archive name AppEvent1035045004.evt.

EventTracker Scheduler Service

The functionality of legacy EventTracker Scheduler service has been enhanced to align with Collection Point architecture.

If you select Standard Console, then the functionality of EventTracker Scheduler service remains unaltered as in earlier versions of EventTracker.

If you select Collection Master or Collection Point Console, then the functionality varies accordingly.

EventTracker Scheduler service monitors and manages EventVault Integrity check schedules. EventTracker logs the service related information in etslog.txt file, which is available in the default EventTracker installation folder typically ...\Program Files\Prism Microsystems\EventTracker and EventVault integrity check related information in CABIntChkLog.txt, which is available in ...\Program Files\Prism Microsystems\EventTracker\Archives folder.

If the ...\Program Files\Prism Microsystems\EventTracker\Archives folder is on a remote machine across the network, crosscheck the following:

EventTracker Scheduler service account settings: Check if the EventTracker Scheduler service account has Administrator privilege on the remote machine. If the EventTracker Scheduler service does not have the mandatory privileges do the following:

1. Open Services.msc
2. Right-click EventTracker Scheduler.
3. From the shortcut menu, choose the Properties option.
4. Click the Log On tab.

5. Select the This account option.

6. Type valid user credentials that has Administrator privilege on the remote machine where the CAB files reside.

7. Click Apply.

Firewall settings (Example: Windows Firewall): When the EventTracker Scheduler service tries to access CAB files on the remote machine, the Firewall may deny access to the remote machine. Allow Firewall to permit EventTracker Scheduler service to access CAB files on the remote machine.

Collection Master and Collection Point communicate through port 14507.

You can also add EventTracker Scheduler service to Exceptions Programs and Services list in Windows Firewall by doing the following:

1. Open Windows Firewall settings window.

2. Click the Exceptions tab.

3. Click Add Program.

4. Click Browse and add the EventTracker Scheduler service to Programs and Services list.
EventTracker Scheduler Service – Collection Master Console

EventTracker Scheduler service at Collection Master Console behaves as a server and will always be in ‘Listen’ mode. Any number of Collection Points could be connected to Collection Master.

EventTracker Scheduler Service – Collection Point Console

EventTracker Scheduler service at Collection Point Console wakes up once in 30 seconds and launches CollectionPointConfig.exe. This exe in turn will query the issdbv3 database for new CAB files to be sent to the Collection Master.
About Archival Process

By default, EventVault Warehouse Manager creates archive files automatically based on two conditions whichever is earlier.

- When the Cache db reaches 50 MB  
  (OR)  
- Once in 24 hours

Each archived file is called as ‘EventBox’.

Archival Process

At the time of archiving the following actions are executed

- A new data table is created at run time.
- All existing events are copied into this newly created data table.
- An SHA1 checksum is generated from this data and stored for future reference.
- This new data table is then compressed into a cabinet file and stored in the configured archive location.

Verify EventVault Integrity

While verifying the integrity of an EventBox, EventVault Warehouse Manager performs the following actions

- The SHA1 checksum of the selected archive is regenerated.
- This new checksum is compared with the older (existing in the database) checksum.
- If the two checksums do not match then an error message is displayed indicating that the data has been tampered.
- If the two checksums match then it means that the data is intact.
1. Select the EventBox(s) from the Available EventBoxes list. 
   (OR) 
   Select the Select All check box to select all EventBoxes. 

2. Click the File menu and select the Verify EventBox option 
   (OR) 
   Click Verify located at the bottom of the console. 

After verifying the integrity, EventVault Warehouse Manager displays the ArchIntegrity report in the Notepad.

![ArchIntegrity - Notepad](image)

---

**Schedule EventVault Integrity Check**

1. Click Configuration on the toolbar. 
   (OR) 

   Click the Options menu and select the Configuration option. 

   EventVault Warehouse Manager displays the Configuration window.
EventTracker EventVault – Introduction and Usage

![Figure 2: Configuration](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EventVault Integrity Check Schedule</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Select this check box to schedule EventVault Integrity check. When you select this check box, EventVault Warehouse Manager will enable Log errors only and Log all actions options. EventVault Integrity check schedule and Event Traffic Analysis schedule are taken care by EventTracker Scheduler service. EventTracker logs two events, 2020 and 2021 for the start and end of Integrity check processes respectively in the Windows Application log.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Select the frequency from this drop-down list. The available options are Daily, Twice Daily and Weekly.</td>
</tr>
<tr>
<td>Log errors only</td>
<td>Select this option to log only error events.</td>
</tr>
<tr>
<td>Log all actions</td>
<td>Select this option for logging both success and failed Integrity check and Extraction of CAB files. EventTracker logs four events, 2016 for failed Integrity check, 2017 for successful Integrity check, 2018 for failed EventBox Extraction and 2014</td>
</tr>
</tbody>
</table>
for successful EventBox Extraction.
If this check box is not selected EventTracker logs two events 2016 and 2018.

<table>
<thead>
<tr>
<th><strong>Time</strong></th>
<th>Select the time from this spin box.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Week Day</strong></td>
<td>This drop-down list is enabled when you select the Frequency as Weekly. This option facilitates on which day of the week you want to start the integrity check.</td>
</tr>
</tbody>
</table>
| **Next Schedule** | Displays the date of schedule. Date depends on the time you enter or select from the Time spin box. The following examples will give you a clear idea.  
Example 1:  
Current system date: 26th Feb 09  
Current system time: 11:00 A.M.  
Frequency: Daily  
If you enter or select past time from the current system time from the Time spin box, EventVault Warehouse Manager will schedule the integrity check for the following day i.e. 27th Feb 09.  
If you enter or select future time from the current system time from the Time spin box, EventVault Warehouse Manager will schedule the integrity check on the same day i.e. 26th Feb 09.  
Example 2:  
Current system date: 26th Feb 09  
Current system time: 11:00 A.M.  
Frequency: Twice Daily  
If you enter or select past time from the current system time from the Time spin box, say for instance 10:30 A.M., EventVault Warehouse Manager will schedule the first integrity check on the same day i.e. 26th Feb 09 10:30 P.M & the second integrity check will be done on the following day i.e. 27th Feb 09 10:30 A.M.  
If you enter or select future time from the current system time from the Time spin box, say for instance 11:30 A.M., EventVault Warehouse Manager will schedule the first integrity check on the same day i.e. 26th Feb 09 11:30 A.M & the second integrity check will be done on the same day i.e. 26th Feb 09 11:30 P.M.  
Example 3:  
Current system date: 26th Feb 09 |
Current system time: 11:00 A.M.
Frequency: Weekly
Day: Friday

If you enter or select past time from the current system time from the
Time spin box, say for instance 10:30 A.M., EventVault Warehouse
Manager will schedule the integrity check for the following week i.e. 5th
Mar 09 10:30 A.M.

If you enter or select future time from the current system time from the
Time spin box, say for instance 11:30 A.M., EventVault Warehouse
Manager will schedule the integrity check for the following week i.e. 5th
Mar 09 11:30 A.M.

Purge Archives

This option helps to purge CAB files after the configured number of days. By default, EventVault
Warehouse Manager retains CAB files for ever.

a. Select the Purge Archives older than check box.

EventVault Warehouse Manager displays the Configuration window with purge frequency.

![Configuration Window]

You can type any number of days to retain the CAB files.
Back up EventVault Data

EventVault data can also be backed up on demand. By backing up to a secure location the data can be retrieved in case the archives are tampered.

1. Select the archive file(s) from the Available EventBoxes list.
   (OR)
   Select the Select All check box to select all the archive files.

2. Click the Options menu and select the Backup Archives option.
   (OR)
   Click Backup Archives on the toolbar.

EventTracker displays EventTracker EventVault Manager message box.

![EventTracker EventVault Manager](image)

3. Click Yes to continue.

   EventTracker displays the Choose Directory window.
4. Select the directory where you want to store the event data.

5. Click **OK**.

   EventTracker displays the ArchIntegrity report in the Notepad after successful completion of backup.
If there is no archive file to back up, EventTracker displays the EventTracker EventVault Manager message box with appropriate message.
Extract and View EventVault Data

1. Select the EventBox(s) from the Available EventBoxes list.
   
   (OR)

   Select the Select All check box to select all the EventBoxes.

2. Click the File menu and select the Extract EventBox option.
   
   (OR)

   Click Extract located at the bottom of the console.

   EventTracker displays the Choose Directory window.

3. Select the directory where you want to store the event data.

4. Click OK.

   After extracting the event data, EventVault Warehouse Manager displays the ArchIntegrity report in the Notepad.
EventTracker EventVault – Introduction and Usage

View Extracted Event Data

- Launch MS Access
- Choose to open an Existing database
- Navigate to the extract directory
- Select the database file (.mdb file)
- Click OK
- View the EventVault data
Delete EventBoxes

1. Select the EventBox(s) from the Available EventBoxes list.
   (OR)
   Select the Select All check box to select all the EventBoxes.

2. Click the File menu and select the Delete EventBox option.
   (OR)
   Click Delete located at the bottom of the console.

   EventTracker displays the Confirm Archive Delete confirmation message box.

3. Click Yes.

   After deleting the EventBox(s), EventVault Warehouse Manager displays the ArchIntegrity report in the Notepad.

Save EventVault Summary Information

This option helps to save the archive summary in a text file.

1. Click the Options menu and select the Save EventBox Metadata option.
   (OR)
   Click Save EventBox Metadata on the toolbar.

   EventTracker displays the Save As window.
2. Type the file name in the **File name** field.

3. Select the directory where you want to store the archive summary.

4. Click **Save**.

## Move Archives

This option helps you to move CAB files to a different location.

1. Select the EventBox(s) from the Available EventBoxes list.

   (OR)

   Select the **Select All** check box to select all the EventBoxes.

2. Click the **File** menu and select the **Move EventBox** option.
(OR)

Click **Move** located at the bottom of the console.

EventVault Warehouse Manager displays the confirmation message box.

![Confirm Archive Move](image1)

**Figure 11: Confirm Archive Move**

3. Click **Yes** to proceed.

EventVault Warehouse Manager displays the Choose Directory window.

![Choose Directory](image2)

**Figure 12: Choose Directory**

4. Select the directory and then click **OK**.

EventTracker moves all the selected files to the new location.
Append Archives

When you manually copy CAB files from different sources to the EventTracker archives folder, you have to recreate the archives index (etwarindex.bin) file with the help of Archive Indexer tool (Control Panel -> Maintenance Tools -> Archive Indexer). This is a very time consuming process if you are copying a huge volume of CAB files.

The Append Archives feature helps you append the Timeticks, name and checksum information about the new CAB files to the existing archive index file with minimal time consumption.

1. Open the EventVault Warehouse Manager.
2. Click Append Archives on the toolbar.

   EventVault Warehouse Manager displays the Append Archives window.
Indicates the CAB files present in the Archives folder. EventVault Warehouse Manager will ignore redundant CAB files.

Indicates that the CAB files are not present in the destination folder i.e. EventTracker Archives folder.

After creating the index file, EventVault Warehouse Manager displays the Append Archives window with actual physical files present in the Archives folder.
Search in Sub Folders check box is selected by default. Clear this check box to append archives in the root folder alone and not in the sub folders.

3. Click and select the path of the folder where you have stored the CAB files.

4. Click OK.

EventVault Warehouse Manager displays the Append Archives window.
You can select individual files by selecting the check boxes against the respective CAB files or collectively by selecting the **Select all missing** cabs.

5. Click **OK**.

EventVault Warehouse Manager displays the progress of appending process.
After the successful completion, EventVault Warehouse Manager displays the ArchiveAppender message box.

![Figure 16]

![Figure 17]
6. Click **OK**.

EventVault Warehouse Manager displays the Append Archives window.

![Append Archives window](image)

EventVault Warehouse Manager appends the cab files to the appropriate folders.
### EventTracker EventVault – Introduction and Usage

**Figure 19: EventVault Warehouse Manager**

<table>
<thead>
<tr>
<th>EventVault Warehouse Manager</th>
<th>File</th>
<th>Options</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vault</td>
<td>Configuration</td>
<td>Save Event</td>
<td>EventVault Metadata</td>
</tr>
</tbody>
</table>

**Available EventBases**

<table>
<thead>
<tr>
<th>Project</th>
<th>Event Type</th>
<th>Description</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker</td>
<td>Event</td>
<td>EventVault Warehouse Manager</td>
<td>C:\Program Files\EventTracker\EventVault\EventVault\14055</td>
</tr>
</tbody>
</table>

---

**EventTracker**

Logging in depth