EventTracker
Secure. Comply. Succeed.

# EventTracker: Backup and Restore Guide

*Version 7.x/8*

Publication Date: Aug 4, 2015

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

# About This Guide

## Abstract

Best practices always advice us to retain periodic backups of all critical applications data. For EventTracker, we recommend you to follow the instructions in this document for effective backup and restore. The frequency of the backup can be decided based on the criticality of the data and configuration for your organisation.

The backup data will be helpful in case of a system crash or accidental loss of data. You can restore the application to its previous state using the latest backup data instead of starting all over again.

## Purpose

The purpose of this document is to guide the EventTracker users in creating a backup of all the data, as well as describing the steps to restore the backup whenever required.

## Intended Audience

Administrator or technical experts who performs the following task:

- Create a backup of EventTracker data/configuration and restore them when required
- Perform maintenance on backups of EventTracker database files

## Scope

The instructions mentioned in this document can be executed on EventTracker v7.5 and later and 8.0.

## Assumptions

This Backup and restore guide assumes that,

- EventTracker is installed and configured as desired
- User is familiar with the various components of EventTracker

**NOTE**: The backup and restoration process will only work for the same versions of EventTracker.

For Example: If the user wants to take a backup of v7.5 database and restore it in v7.6, the backup and restoration process fails.

# Table of Contents

# Automated method to take a backup of the database

## Process of Backup

a) Create a backup folder named 'BackupID' (where ID can be a unique value or a date that will help tabulating the backup) to store the backup files.

b) Create a sub folder named Common under BackupID folder.

Now,

a) Double-click **EventTracker Control Panel**, double-click **Diagnostics**.

b) Click the **Backup** button.

Backup & Restore window displays.

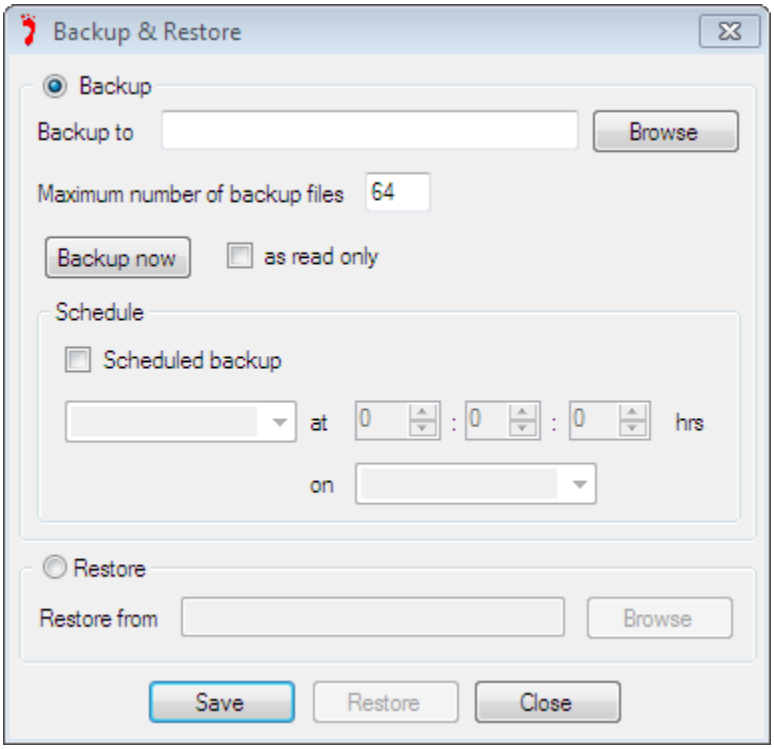


Figure 1

c) Browse and select the backup folder named 'BackupID' to backup data.

d) Click the **Backup now** button.

This takes a backup of *.mdb, *.mdf and *.ldf files only.

After the backup has been taken, go to folder for which the backup has been taken. A file with the extension .bkp will be used to restore later.

# Manual method to take a backup of the database

## Before you start

- Please login to the EventTracker console to verify that installation is a success and that the configuration is as desired.
- Please ensure that no reports or analyses are running. This can be done by verifying task manager. Right click on the task bar, click **Task manager**, and then click the **Processes** tab.
- Verify the processes and make sure that 'Prism.Reports.ServiceProcessor.exe' is not running.

## Process of Backup

1. Stop all the EventTracker Services in exactly the same order as listed below.
2. To view **Services**, click the **Start** button, and then select **Control Panel**.
3. Select **Administrative Tools**, and then select **Services**.
    - EventTracker Agent
    - EventTracker Scheduler
    - EventTracker Alerter
    - EventTracker EventVault
    - EventTracker Indexer
    - EventTracker Receiver
    - EventTracker Remoting
    - EventTracker Reporter
    - StatusTracker (If StatusTracker Is installed)
    - WcwService (If Change Audit is installed)
    - TrapTracker Receiver (If TrapTracker is installed)
    - Event Correlator (If Correlator update is installed)
4. Stop **SQL Express/Server** service.
5. Ensure that all the services mentioned in step 3 and 4 have stopped successfully.

6. Create a backup folder named 'BackupID' (where ID can be a unique value or a date that will help tabulating the backup) to store the backup files.
7. Create a sub folder named Common under BackupID folder.
8. Go to the <installdir>\Common folder.

   <Installdir> is the full path of the directory where EventTracker is installed.
9. From the above folder copy the *.mdf and *.ldf files, and store them in the Common sub folder under the 'BackupID' folder.

**NOTE**: If the user is using Collection Master, copy the Sites_DB file in the Common sub folder under the 'BackupID' folder. **(This is only for v8.0 which will contain the behavior data).**

## Common steps for both the Automated & Manual backup:

1. Create a sub folder named EventTracker under BackupID folder.
2. From the <installdir>\EventTracker, copy the following folders/Files to the 'BackupID' folder.
   - Archives
   - Reports
   - Alerts
   - Cache
   - DLA
   - AgentConfig
   - SCAP (If Configuration Assessment is configured)
   - All the files with .ini extension
   - All the files with .etw extension
3. Create a sub folder named TrapTracker under BackupID folder.
4. From the <installdir>\TrapTracker copy the following files to the <BackupID>\TrapTracker folder
   - mymibs.bin
   - All files with .ini extension
5. Create a sub folder named WCWindows under BackupID folder.

6. From the <installdir>\WCWindows copy the following folders to the <BackupID>\WCWindows folder
   - Policies
   - SnapShots
   - All files with .ini extension
7. In the <BackupID> folder, create a subfolder named Agent under EventTracker sub folder.

8. From the <installdir>\EventTracker\Agent, copy the following folders to the <BackupID>\EventTracker\Agent folder
   - SCAP
   - Script
   - All files with .ini extension
   - All files with .bin extension
   - .p12 file if Checkpoint LFM configured
9. Start all the services which were stopped in step 3 and step 4.

   Now the EventTracker application is ready to process the new data.

If the user has used custom logo,

10. Create a sub folder named EventTrackerWeb\images under BackupID folder and copy the CustomLogos folder to <installdir>\EventTrackerWeb\images\

## NOTE:

For the BackupID folder, maintain the same sub folder structure as in the installed directory. This will be helpful during restore. The hierarchical view of BackupID folder is given below.

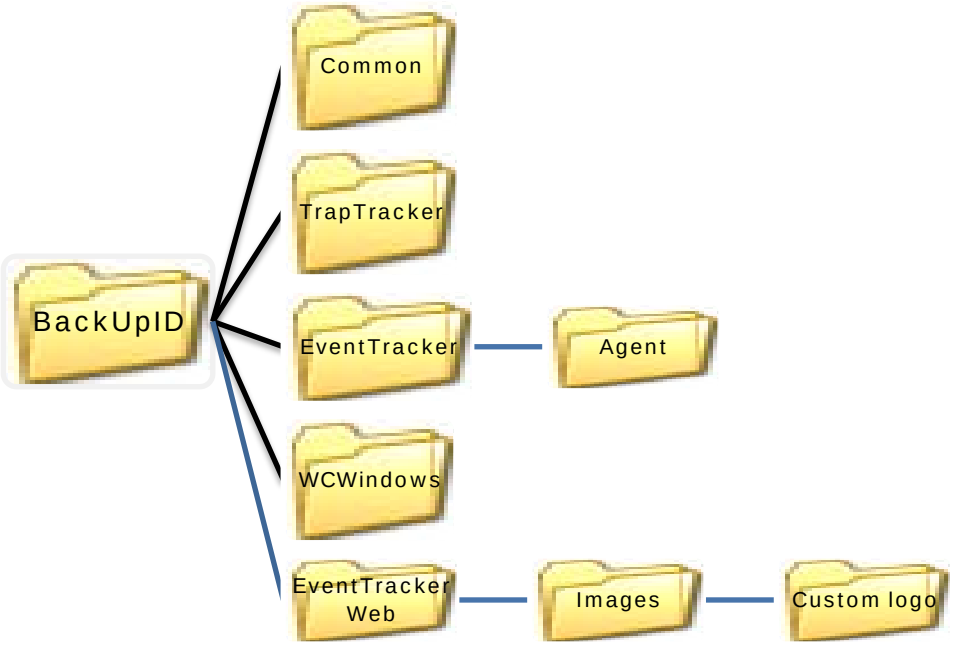


Figure 2

# Process of Restoration

## Automated Database Restoration:

To restore the backup file,

a) Select the Restore option.

b) Browse and select the relevant folder(s) to restore data.

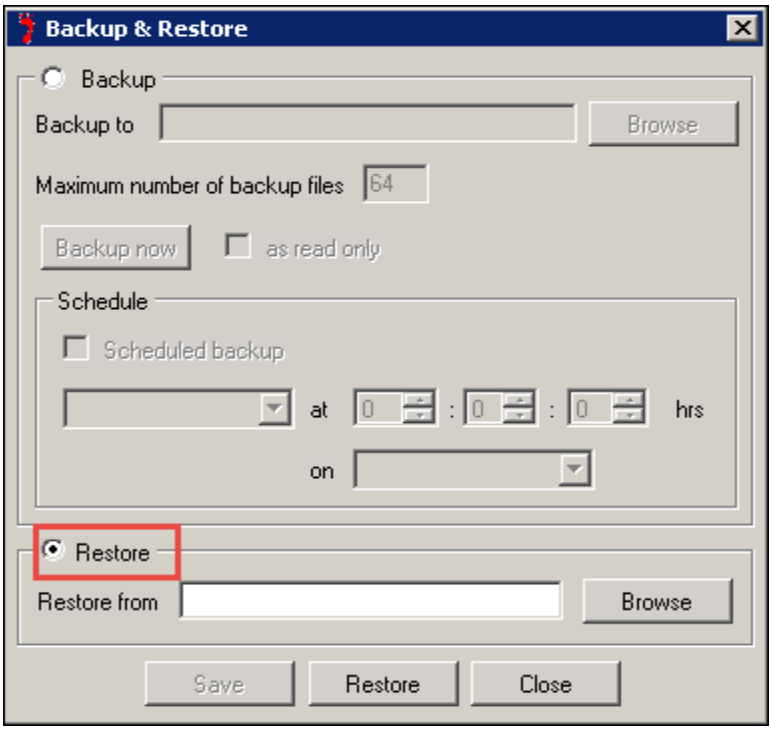


Figure 3

c) Click the **Restore** button.

A warning message displays.

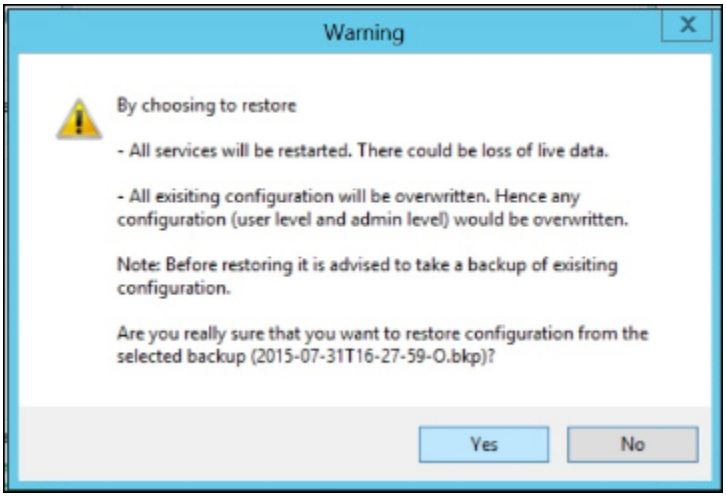


Figure 4

d) Click the **Yes** button.

The restoration process starts.


Figure 5

e) A confirmation message is displayed once the restoration process is completed.

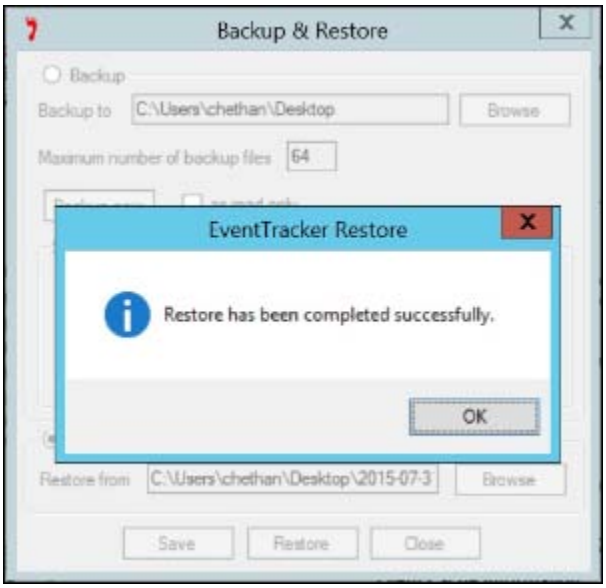


Figure 6

f) Click **OK.**

# Manual Database Restoration:

## Before you start

- Please ensure that no reports or analyses are running. This can be done by verifying task manager. Right click on the task bar, click **Task manager**, and then click the **Processes** tab.
- Verify the processes and make sure that 'Prism.Reports.ServiceProcessor.exe' is not running.
- While restoring from a backup please ensure that it is restored to the,
  - Same version from which the backup was made
  - Same EventTracker patches applied that were present during the backup
  - Same OS version and architecture (32 bit/64 bit)
- If the EventTracker is already installed on your machine, then skip the first step of restore process.

## Restore data

1. Install EventTracker with the same version and all the patches that were applied earlier.
2. Stop all the **EventTracker Services** in exactly the same order as listed below.
   - EventTracker Agent
   - EventTracker Scheduler
   - EventTracker Alerter
   - EventTracker EventVault
   - EventTracker Indexer
   - EventTracker Receiver
   - EventTracker Remoting
   - EventTracker Reporter
   - StatusTracker (If StatusTracker Is installed)
   - WcwService (If Change Audit is installed)
   - TrapTracker Receiver (If TrapTracker is installed)
   - Event Correlator (If Correlator update is installed)
3. Stop **SQL Express/Server** service.
4. Ensure that all the services mentioned in step 2 & 3 have stopped successfully.
5. Now you need to copy all the restored folder and files saved in <BackupID>\Common folder to <installdir>\Common folder.

a. Copy the *.mdf and *.ldf files from the <BackupID>\Common folder and replace them under <installdir>\Common folder.

**NOTE**: If user is using Collection Master, copy the Sites_DB file from the <BackupID>\Common folder and replace them under <installdir>\Common folder.. **(This applies to the v8.0).**

## Common steps for both Automated & Manual restoration:

a. Copy the following folders from the BackupID>\EventTracker folder and replace them under <installdir>\EventTracker
   - Archives
   - Reports
   - Alerts
   - Cache
   - DLA
   - AgentConfig
   - SCAP (If Configuration Assessment is configured)
   - All the files with .ini extension
   - All the files with .etw extension

b. Copy the following folders from the BackupID>\TrapTracker folder and replace them under <installdir>\TrapTracker
   - Mymibs.bin
   - All files with .ini extension

c. Copy the following folders from the BackupID>\WCWindows folder and replace them under <installdir>\WCWindows
   - Policies
   - SnapShots
   - All files with .ini extension

d. Copy the following folders from the <Installdir>\EventTracker\Agent folder and replace them under <BackupID>\EventTracker\Agent folder
   - SCAP

- Script
- All files with .ini extension
- All files with .bin extension
- .p12 file if Checkpoint LFM configured

f. If you are using the custom logo, copy the following folder from the <BackupID>\EventTrackerWeb\images\folder and replace them under <installdir>\EventTrackerWeb\images\folder.CustomLogos

1. Start all the services, which were stopped in step 2 & 3.

   Now the EventTracker server has been restored using the backup data from 'BackupID' and is ready for use (reporting, search and analysis).