System Transfer Guide

Transferring EventTracker Manager to a new system

Publication Date: Aug 6, 2014

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

Abstract

Transfer of EventTracker Manager from existing system to new system may be necessitated due to many possible reasons, like if the system is running out of hard disk space or installing a newer version in the new system.

Purpose

The purpose of this document is to help users transfer EventTracker Manager from existing system to new system, and to verify the expected functionality and performance of all its components. If you encounter any problems during the transfer process, please contact Support to get quick and thorough instructions.

Audience

EventTracker users like 'Administrators' or 'Technical experts' who wish to transfer EventTracker Manager from existing system to new system.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

Instructions for Advanced User

The Quick steps to transfer EventTracker Manager from existing system to new system:

1. Install EventTracker Manager (Same or newer version) on a new system
2. Update all EventTracker Agents to point to the new Manager
3. Transfer data from the **existing system** to the **new system**
4. Update all Change Audit Agents to point to new Manager
5. Verify the agent status in System Manager

Detailed Instructions

Install the EventTracker manager on a new system

Settings for the 'New manager' system:

1. Install the same or newer version of EventTracker.
2. Verify that all the EventTracker services are running.
3. Open the EventTracker web console, and check if events are being received.

   For detailed installation instructions, please refer EventTracker Installation Guide for respective versions.

Update all EventTracker agents to point to the new manager

Agents which are sending events to existing manager needs to be re-configured to send the events to the new manager. How to change the EventTracker manager is well described with the help of the given scenario.

Scenario: In the following example, we have described how to point all the agents, which are sending events to 'Mcloon' (the existing manager) to send all events to system 'ELC' (new manager).

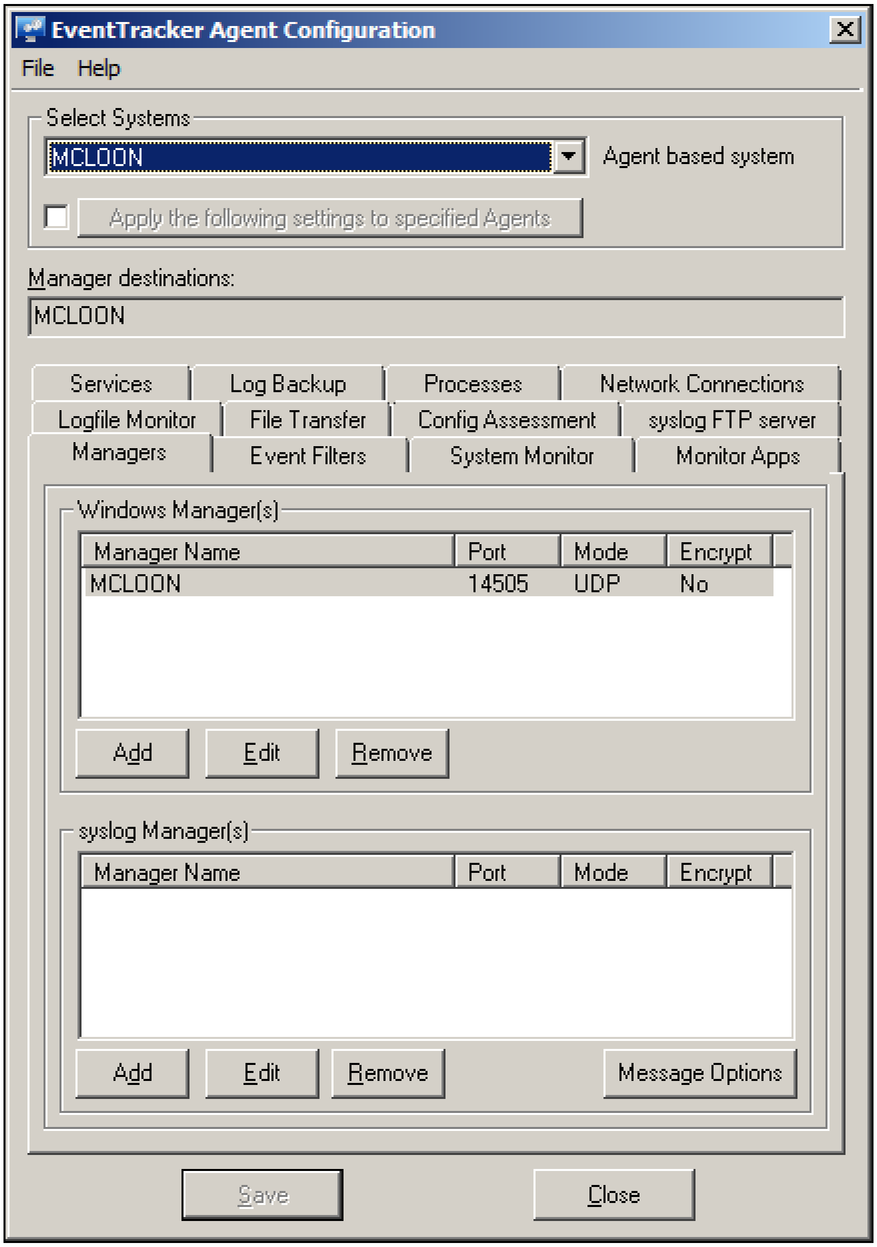
Assumption:

- MCLOON has deployed agents to ESXSERVER and SAFARI.

Settings for existing manager system:

1. Open **EventTracker Control Panel**, and then double click **EventTracker Agent Configuration**.

   EventTracker displays the '**EventTracker Agent Configuration'** dialog box. (Refer Figure 1)



Select Systems: MCLOON

Agent based system

Manager destinations: MCLOON

Windows Manager(s)

Manager Name	Port	Mode	Encrypt
MCLOON	14505	UDP	No

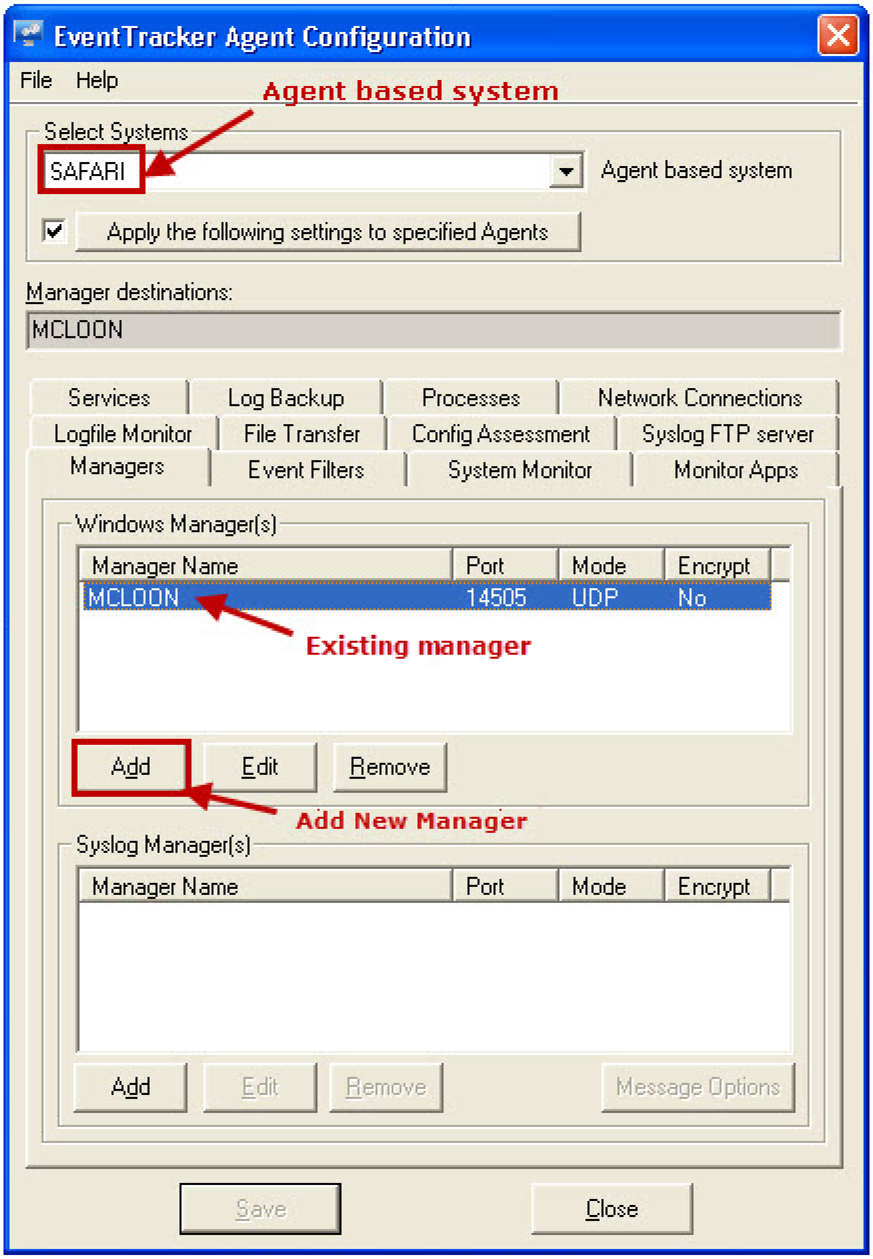
syslog Manager(s)

Manager Name	Port	Mode	Encrypt

Figure 1

2. Select a system from the **Select Systems** drop-down list, which is reporting to ‘Mcloon’.

   For example: SAFARI



Select Systems: SAFARI ▾ Agent based system

☑ Apply the following settings to specified Agents

Manager destinations: MCLOON

Windows Manager(s)

Manager Name	Port	Mode	Encrypt
MCLOON	14505	UDP	No

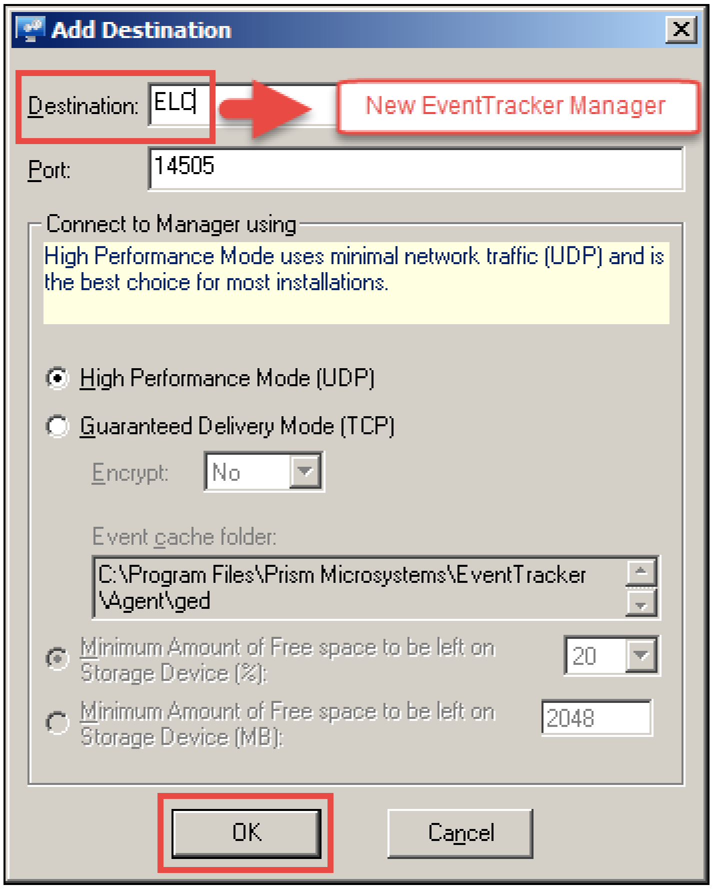
Syslog Manager(s)

Manager Name	Port	Mode	Encrypt

Figure 2

3. Click the **Add** button.

   EventTracker displays the **Add Destination** dialog box. (Refer Figure 3)



Destination: ELC

Port: 14505

Connect to Manager using

High Performance Mode uses minimal network traffic (UDP) and is the best choice for most installations.

● High Performance Mode (UDP)

○ Guaranteed Delivery Mode (TCP)

Encrypt: No

Event cache folder:

C:\Program Files\Prism Microsystems\EventTracker \Agent\ged

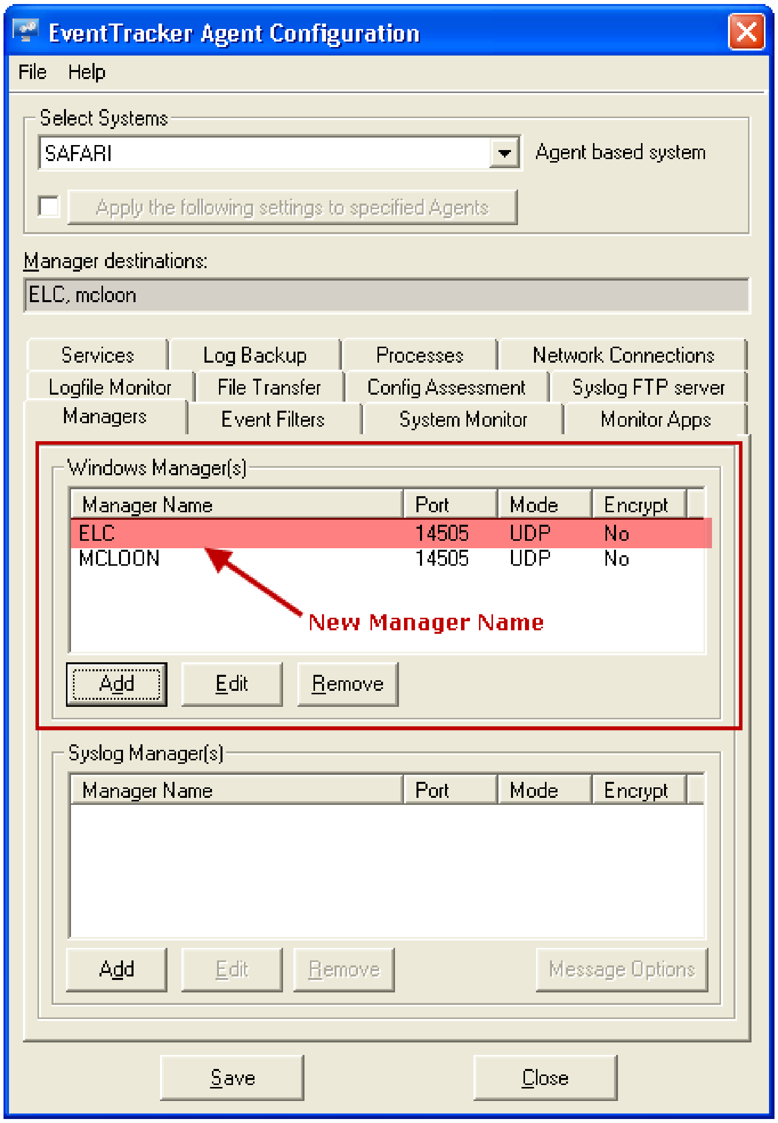
● Minimum Amount of Free space to be left on Storage Device (%): 20

○ Minimum Amount of Free space to be left on Storage Device (MB): 2048

Figure 3: Add Destination

4. Enter the name of the new manager in the **Destination** field.
5. Click the **OK** button.

   EventTracker displays the new manager name in the 'Windows Manager(s)' pane.



Select Systems: SAFARI

Agent based system

□ Apply the following settings to specified Agents

Manager destinations: ELC, mcloon

Windows Manager(s)

Manager Name	Port	Mode	Encrypt
ELC	14505	UDP	No
MCLOON	14505	UDP	No

Syslog Manager(s)

Manager Name	Port	Mode	Encrypt

Figure 4

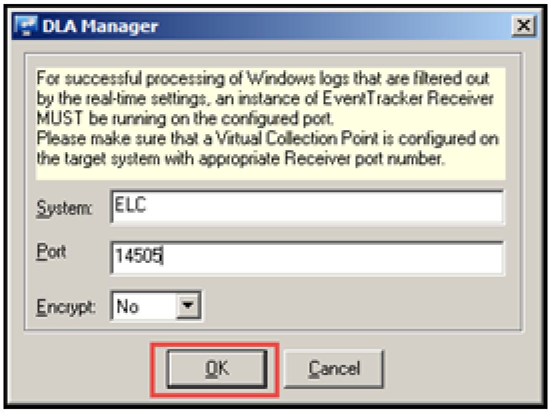
6. Select the existing manager (i.e. Mcloon), and then click the **Remove** button.

   EventTracker removes the existing manager name from the list.

   NOTE:

   You can keep both the managers in the list.

7. Click the **File Transfer** tab, and click the **Add** button.
8. In the **DLA manager** dialog box, enter the new manager's name in the **System** box.
9. Make required selection in **Encrypt** dropdown.



DLA Manager

For successful processing of Windows logs that are filtered out by the real-time settings, an instance of EventTracker Receiver MUST be running on the configured port.
Please make sure that a Virtual Collection Point is configured on the target system with appropriate Receiver port number.

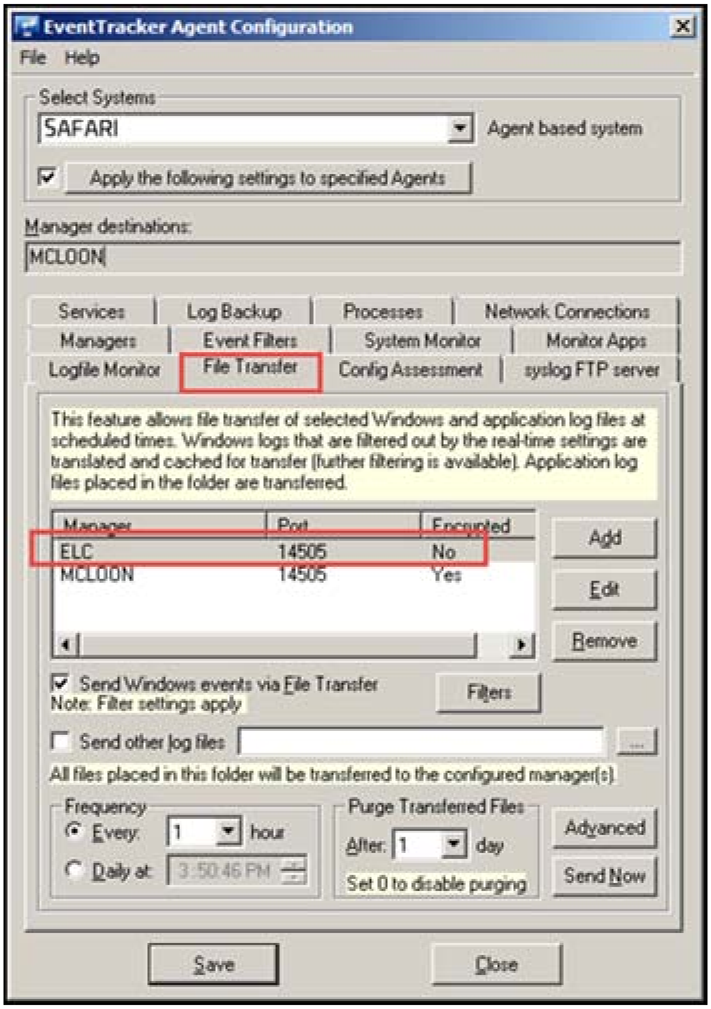
System: ELC

Port: 14505

Encrypt: No

Figure 5

10. Click the **OK** button.



EventTracker Agent Configuration

Select Systems: SAFARI — Agent based system

☑ Apply the following settings to specified Agents

Manager destinations: MCLOON

This feature allows file transfer of selected Windows and application log files at scheduled times. Windows logs that are filtered out by the real-time settings are translated and cached for transfer (further filtering is available). Application log files placed in the folder are transferred.

Manager	Port	Encrypted
ELC	14505	No
MCLOON	14505	Yes

☑ Send Windows events via File Transfer
Note: Filter settings apply

☐ Send other log files

All files placed in this folder will be transferred to the configured manager(s).

Frequency: ● Every: 1 hour; ○ Daily at: 3:50:46 PM

Purge Transferred Files: After: 1 day. Set 0 to disable purging

Figure 6

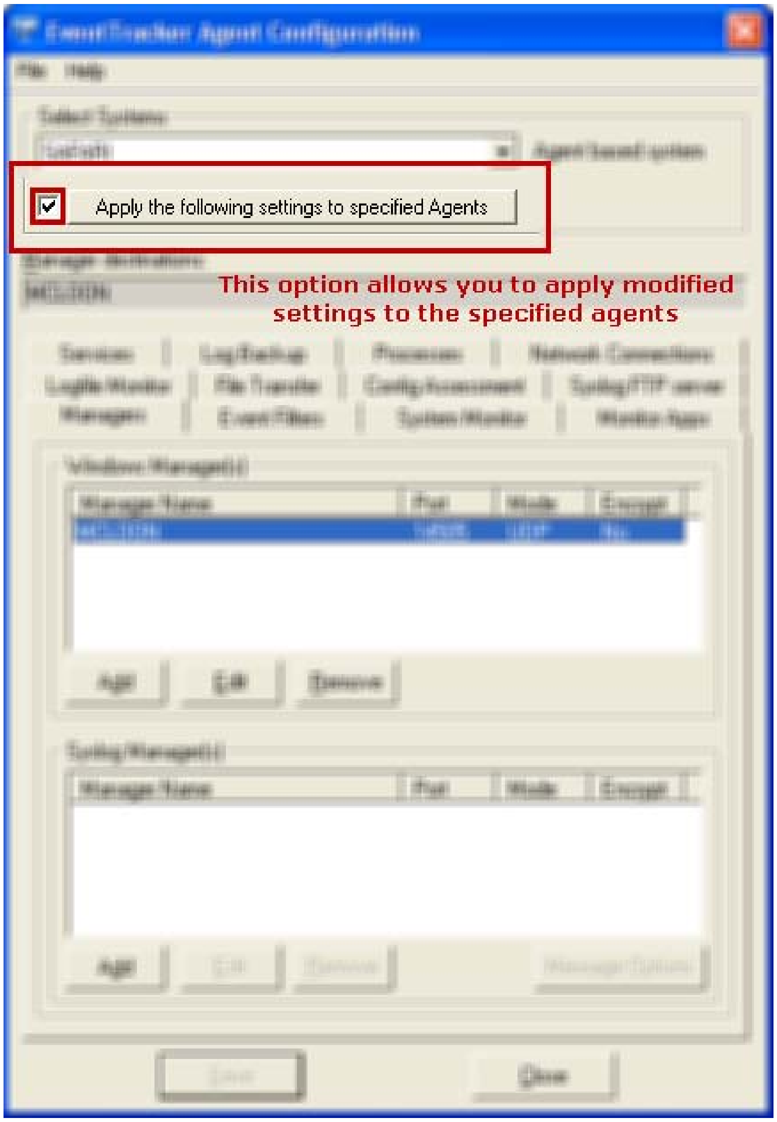
11. Select the existing manager (i.e. Mcloon), and click the **Remove** button.

    EventTracker removes the existing manager name from the list.

    NOTE:

    You can keep both the managers in the list.

12. Click the **Save** button to save the configurations made in **Manager** and **File Transfer** tabs.
13. Click the check box, and select the **Apply the following settings to specified clients** button.

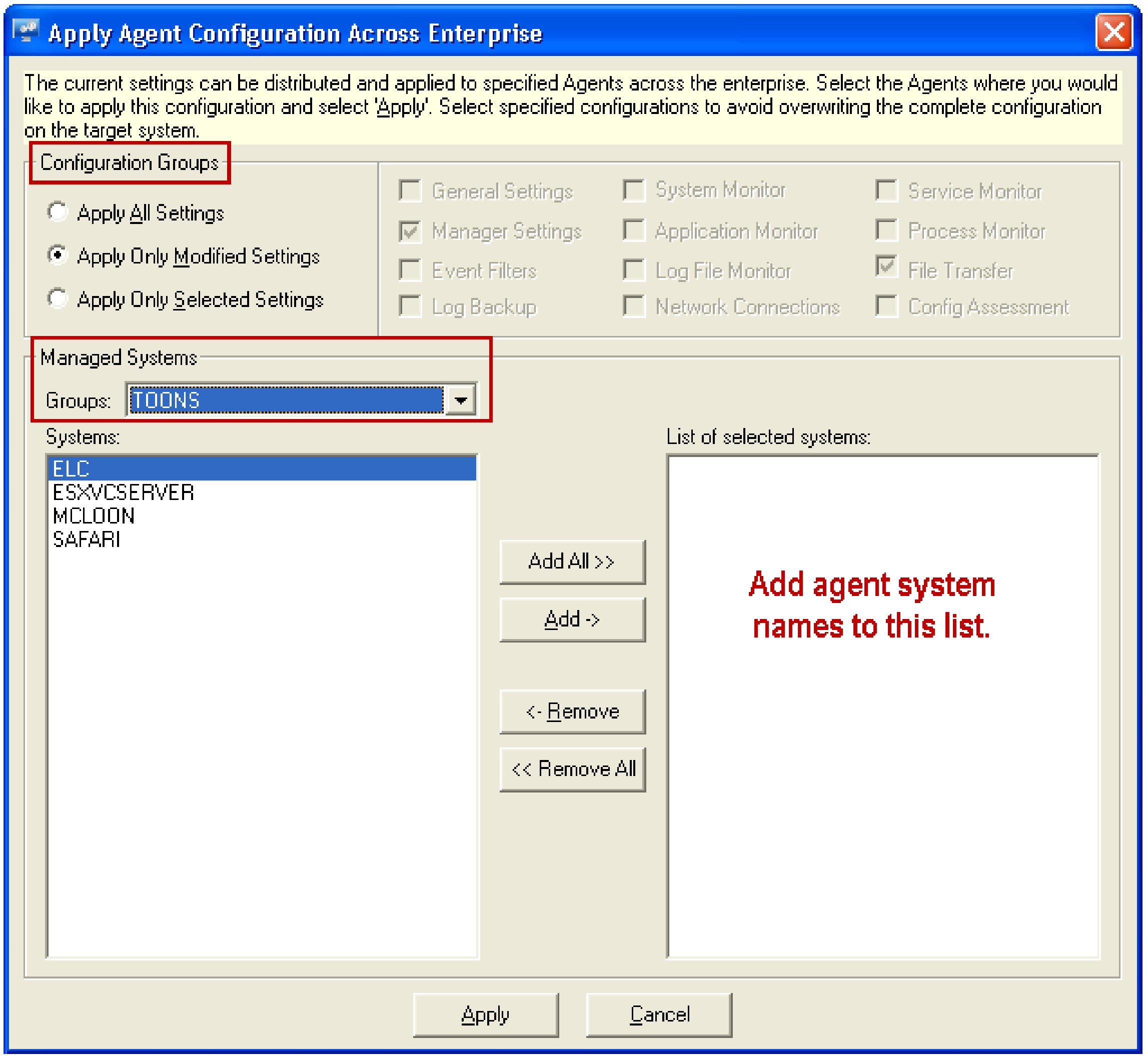


☑ Apply the following settings to specified Agents

This option allows you to apply modified settings to the specified agents

Figure 7

EventTracker displays '**Apply Agent Configuration Across Enterprise**' dialog box. (Refer Figure 6).



Apply Agent Configuration Across Enterprise

The current settings can be distributed and applied to specified Agents across the enterprise. Select the Agents where you would like to apply this configuration and select 'Apply'. Select specified configurations to avoid overwriting the complete configuration on the target system.

Configuration Groups

○ Apply All Settings
● Apply Only Modified Settings
○ Apply Only Selected Settings

□ General Settings	□ System Monitor	□ Service Monitor
☑ Manager Settings	□ Application Monitor	□ Process Monitor
□ Event Filters	□ Log File Monitor	☑ File Transfer
□ Log Backup	□ Network Connections	□ Config Assessment

Managed Systems

Groups: TOONS

Systems:

ELC
ESXVCSERVER
MCLOON
SAFARI

List of selected systems:

Add agent system names to this list.

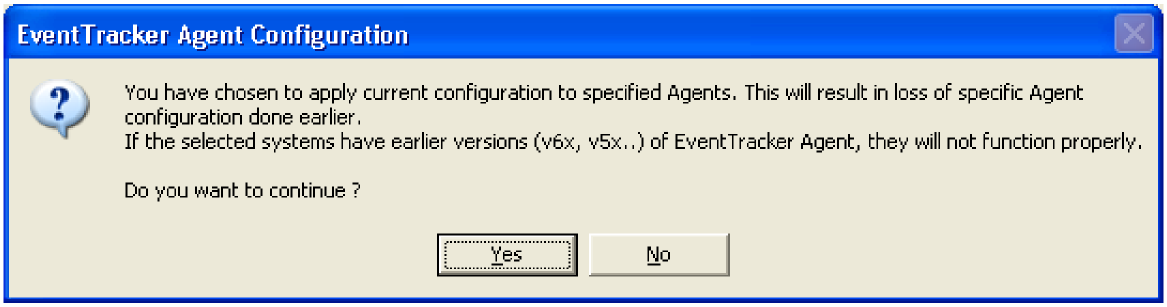
Figure 8: Apply Agent Configuration Across Enterprise

14. In the **Configuration Groups** pane, select '**Apply Only Modified Settings**' option.

    Selecting this option will only change the 'Manager System' name and retain the old configuration settings for the agents.

15. From the **Groups** dropdown, select the group name where the agent systems are present.
16. In the **Systems** list, select the agent name, and then click the **Add >>** button to add the agent or click **Add All >>** button to add all the agents to the **List of selected systems**
17. Click the **Apply** button.

    EventTracker displays a warning message. (Refer Figure 7)



You have chosen to apply current configuration to specified Agents. This will result in loss of specific Agent configuration done earlier.
If the selected systems have earlier versions (v6x, v5x..) of EventTracker Agent, they will not function properly.

Do you want to continue ?

Figure 9

18. Click **Yes**, and then click the **Close** button.

NOTE:

You can skip this step if you are retaining the existing manager system name.

Data transfer from the existing system to the new system

Same version and same path

If the same version of EventTracker is installed on the same path as the existing system (i.e. The OS architecture is same) (32 Bit to 32 Bit), then follow the instructions for backup and restore as stated below:

Process of backup from 'Existing manager server':

Before you start

- 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.
- The backup folder should be accessible to the new manager system, therefore save it in a shared medium.

Backing up data

1. Stop all the 'EventTracker Services' in exactly the same order as listed below.

   Services can be accessed from **Start**-> **Control Panel**-> **Administrative Tools**-> **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)

2. Stop **SQL Express/Server** service.
3. Ensure that all the services mentioned in step 1 and 2 have stopped successfully.
4. In the shared medium, create a backup folder named 'BackupID' to store the backup files.

   Here, 'ID' can be a unique value or a date that will help tabulating the backup.
5. Create a sub folder named Common under BackupID folder.
6. Go to the <installdir>\Common folder.

   <Installdir> is the full path of the directory where EventTracker is installed.
7. From the above folder copy the *.mdf and *.ldf files, and store them in the newly created Common sub folder under the 'BackupID' folder.
8. Create a sub folder named EventTracker under BackupID folder.
9. From the <installdir>\EventTracker, copy the following folders/files to the 'BackupID' folder.

   - Archives
   - Reports
   - Alerts
   - Cache
   - DLA
   - AgentConfig
   - Benchmarks
   - SCAP (If 'Configuration Assessment' is configured)
   - All the files with .ini extension

- All the files with .etw extension

10. From the <installdir>\TrapTracker copy the following files to the <BackupID>\TrapTracker folder

    - mymibs.bin
    - All files with .ini extension

11. From the <installdir>\WCWindows copy the following folders to the <BackupID>\WCWindows folder

    - Policies
    - SnapShots
    - All files with .ini extension

12. In the <BackupID> folder, create a subfolder named Agent under EventTracker sub folder.

13. 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

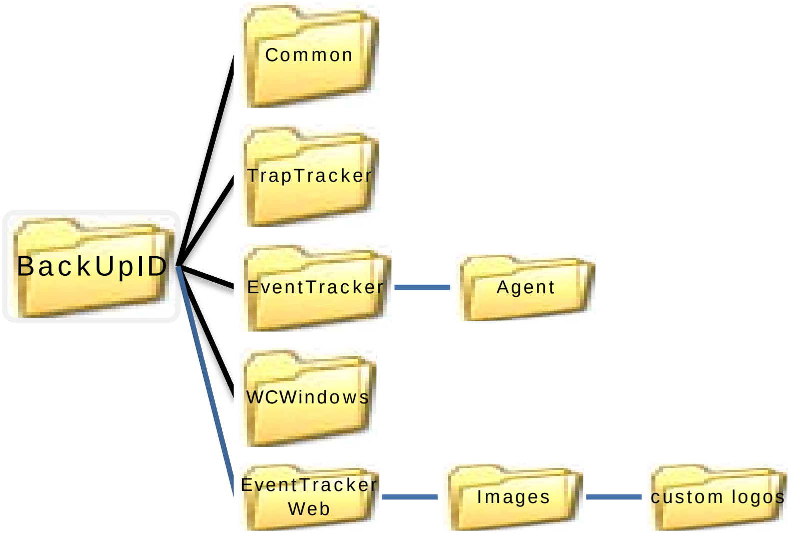
14. Start all the services which were stopped in step1 and 2.

If the user has used a custom logo,

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



Process of restoration on 'New manager server':

Before you start

- Please ensure that no reports or analysis 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 updates applied that were present during the backup
  - ➢ Same OS version and architecture (32 bit/64 bit)

Restoring the data on new manager system:

1. 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 is installed)

2. Stop **SQL Express/Server service**.
3. Ensure that all the services mentioned in step 1 & 2 have stopped successfully.
4. Now you need to replace the files and folders present under <installdir> with those present in <BackupID> of shared medium.

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

b. Copy the following folders from the <BackupID>\EventTracker folder, and replace them under <installdir>\EventTracker.

- Archives
- Reports
- Alerts
- Cache
- DLA

- AgentConfig
- Benchmarks
- SCAP (If Configuration Assessment is configured)
- All the files with .ini extension
- All the files with .etw extension

c. Copy the following files from the <BackupID>\TrapTracker folder, and replace them under <installdir>\TrapTracker.

- mymibs.bin
- All files with .ini extension

d. Copy the following folders from the <BackupID>\WCWindows folder, and replace them under <installdir>\WCWindows.

- Policies
- SnapShots
- All files with .ini extension

e. Copy the following folders from <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

For users using custom logos,

f. Copy the following folder from the <installdir>\EventTrackerWeb\images\folder and replace them under <BackupID>\EventTrackerWeb\images\folder.CustomLogos

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

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

Same version and different path

If the same version of EventTracker is installed on a different path as the existing system (i.e. The OS architecture is different or install path is different) (32 Bit to 64 Bit or from C:\ to D:\), then follow the instructions for backup and restore as stated below:

Process of backup from 'Existing manager server':

Before you start

- 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.
- The backup folder should be accessible to the new manager system, therefore save it in a shared medium.

Backing up data

1. Stop all the 'EventTracker Services' in exactly the same order as listed below.

   Services can be accessed from **Start**-> **Control Panel**-> **Administrative Tools**-> **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)

2. Stop SQL Express/Server service.
3. Ensure that all the services mentioned in step 1 and 2 have stopped successfully.
4. In the shared medium, create a backup folder named 'BackupID' to store the backup files.

   Here, 'ID' can be a unique value or a date that will help tabulating the backup.
5. Create a sub folder named Common under BackupID folder.
6. Go to the <installdir>\Common folder.

   <Installdir> is the full path of the directory where EventTracker is installed.
7. From the above folder copy the *.mdf and *.ldf files, and store them in the newly created Common sub folder under the 'BackupID' folder.
8. Create a sub folder named EventTracker under BackupID folder.
9. From the <installdir>\EventTracker, copy the following folders/files to the 'BackupID' folder.
   - Archives
   - Reports

- Alerts
- Cache
- DLA
- AgentConfig
- Benchmarks
- SCAP (If 'Configuration Assessment' is configured)
- All the files with .etw extension

10. From the <installdir>\TrapTracker copy the following files to the <BackupID>\TrapTracker folder

    - mymibs.bin
    - All files with .ini extension

11. From the <installdir>\WCWindows copy the following folders to the <BackupID>\WCWindows folder

    - Policies
    - SnapShots
    - All files with .ini extension

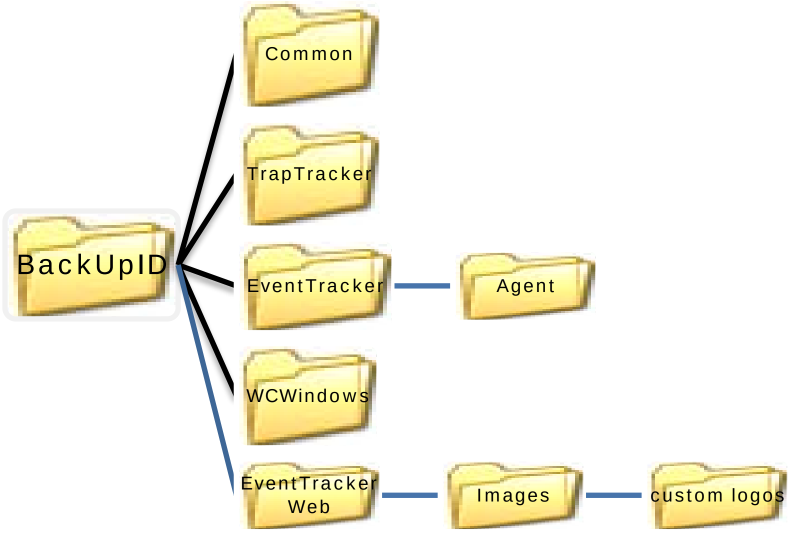
12. Start all the services which were stopped in step 1and 2.

If the user has used a custom logo,

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



Process of restoration on 'New manager server':

Before you start

- Please ensure that no reports or analysis 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 updates applied that were present during the backup

Restoring the data on new manager system:

1. 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 is installed)

2. Stop **SQL Express/Server** service.
3. Ensure that all the services mentioned in step 1 & 2 have stopped successfully.
4. Now you need to replace the files and folders present under <installdir> with those present in <BackupID> of shared medium.

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

2. Copy the following folders from the <BackupID>\EventTracker folder, and replace them under <installdir>\EventTracker.
    - Archives
    - Reports
    - Alerts
    - Cache
    - DLA
    - AgentConfig

- Benchmarks
- SCAP (If Configuration Assessment is configured)
- All the files with .etw extension

3. Copy the following files from the <BackupID>\TrapTracker folder, and replace them under <installdir>\TrapTracker.

    - mymibs.bin
    - All files with .ini extension

4. Copy the following folders from the <BackupID>\WCWindows folder, and replace them under <installdir>\WCWindows.

    - Policies
    - SnapShots
    - All files with .ini extension

For users using custom logos,

f. Copy the following folder from the <installdir>\EventTrackerWeb\images\folder and replace them under <BackupID>\EventTrackerWeb\images\folder.CustomLogos

5. Start **SQL Express/Server service**.

6. Run the following batch files:

    a. Changearchivepath.bat

    b. Changegeneratedreportpath.bat

    c. Changingtblconfig.bat

    d. Changeparserspath.bat

    e. ChangeBenchmarkspath.bat

f. ChangeResultspath.bat

g. ChangeClientDetailpath.bat (Run on CM when CP's are reporting)

NOTE:

The path needs to be modified in the batch files.

7. Start all the services, which were stopped in step 1.

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

Different version and same path

If a different version of EventTracker is installed on the same path as the existing system (i.e. The OS architecture is same) (32 Bit to 32 Bit), then follow the instructions for backup and restore as stated below

Process of backup from 'Existing manager server':

Before you start

- 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.
- The backup folder should be accessible to the new manager system, therefore save it in a shared medium.

Backing up data

1. Backup all custom Categories, Alerts (Please check the 'Export E-mail Settings" check box), Filters, Scheduled Reports and RSS Feeds using Export Import Utility
2. Stop all the 'EventTracker Services' in exactly the same order as listed below.

   Services can be accessed from **Start**-> **Control Panel**-> **Administrative Tools**-> **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)

3. Stop SQL Express/Server service.
4. Ensure that all the services mentioned in step 2 and 3 have stopped successfully.
5. In the shared medium, create a backup folder named 'BackupID' to store the backup files.

   Here, 'ID' can be a unique value or a date that will help tabulating the backup.
6. Create a sub folder named Common under BackupID folder.
7. Go to the <installdir>\Common folder.

   <Installdir> is the full path of the directory where EventTracker is installed.
8. From the above folder copy the *.mdf and *.ldf files, and store them in the newly created Common sub folder under the 'BackupID' folder.
9. Create a sub folder named EventTracker under BackupID folder.
10. 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 .etw extension

11. From the <installdir>\TrapTracker copy the following files to the <BackupID>\TrapTracker folder

    - mymibs.bin
    - All files with .ini extension

12. From the <installdir>\WCWindows copy the following folders to the <BackupID>\WCWindows folder

    - Policies
    - SnapShots
    - All files with .ini extension

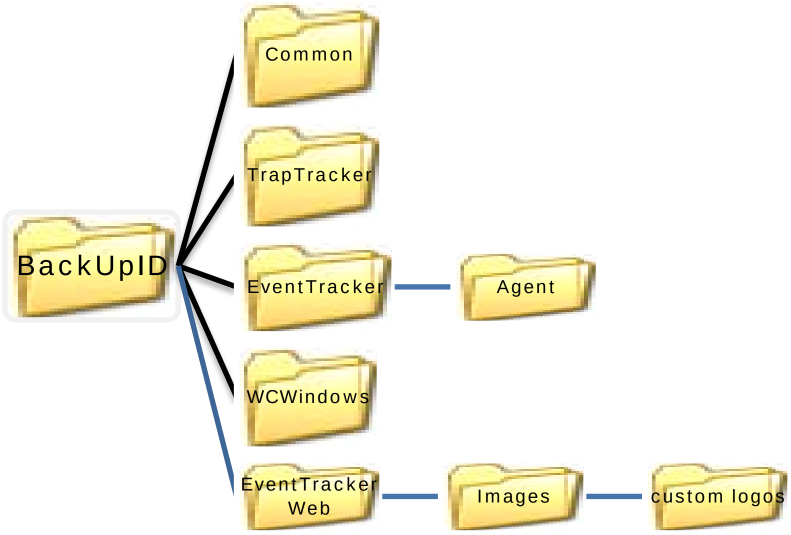
13. Start all the services which were stopped in step 2 and 3.

If the user has used the custom logo,

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



Process of restoration on 'New manager server':

Before you start

- Please ensure that no reports or analysis 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 OS version and architecture (32 bit/64 bit)

Restoring the data on new manager system:

1. 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 is installed)

2. Stop **SQL Express/Server** service.
3. Ensure that all the services mentioned in step 1 & 2 have stopped successfully.
4. Create a folder 'EventTrackerDB' in C:\ drive.
5. Copy the *.mdf and *.ldf files from the <BackupID>\Common folder to 'EventTrackerDB' folder created in step 4.
6. Now you need to replace the files and folders present under <installdir> with those present in <BackupID> of shared medium.

1. 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 .etw extension

2. Copy the following files from the <BackupID>\TrapTracker folder, and replace them under <installdir>\TrapTracker.

   - mymibs.bin
   - All files with .ini extension

3. Copy the following folders from the <BackupID>\WCWindows folder, and replace them under <installdir>\WCWindows.

   - Policies
   - SnapShots
   - All files with .ini extension

For users using custom logos,

f. Copy the following folder from the <installdir>\EventTrackerWeb\images\folder and replace them under <BackupID>\EventTrackerWeb\images\folder.CustomLogos

7. Start **SQL Express/Server** service.

8. Rename the 'Reports' folder which is copied in step 6.1 to 'Previous Version Reports'.

9. Run 'Setpreviousreportpath.bat' batch file.

10. Run 'ImportCabReportDetails.bat' batch file.

11. Run 'ImportClienttDetails.bat' batch file. (Should be run on Collection Master)

12. Run 'Changepreviousgeneratedreportpath.bat' batch file.

13. Import all custom Categories, Alerts (Please check the 'Export E-mail Settings' check box), Filters, Scheduled Reports and RSS Feeds using Export Import Utility

14. Start all the services, which were stopped in step 1.

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

Different version and different path

If a different version of EventTracker is installed on a different path as the existing system (i.e. The OS architecture is different or install path is different) (32 Bit to 64 Bit or from C:\ to D:\), then follow the instructions for backup and restore as stated below:

Process of backup from 'Existing manager server':

Before you start

- 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.
- The backup folder should be accessible to the new manager system, therefore save it in a shared medium.

Backing up data

1. Backup all custom Categories, Alerts (Please check the 'Export E-mail Settings" check box), Filters, Scheduled Reports and RSS Feeds using Export Import Utility
2. Stop all the 'EventTracker Services' in exactly the same order as listed below.

   Services can be accessed from **Start** -> **Control Panel** -> **Administrative Tools** -> **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)

3. Stop SQL Express/Server service.
4. Ensure that all the services mentioned in step 2 and 3 have stopped successfully.
5. In the shared medium, create a backup folder named 'BackupID' to store the backup files.

   Here, 'ID' can be a unique value or a date that will help tabulating the backup.
6. Create a sub folder named Common under BackupID folder.
7. Go to the <installdir>\Common folder.

   <Installdir> is the full path of the directory where EventTracker is installed.
8. From the above folder copy the *.mdf and *.ldf files, and store them in the newly created Common sub folder under the 'BackupID' folder.
9. Create a sub folder named EventTracker under BackupID folder.
10. 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 .etw extension
11. From the <installdir>\TrapTracker copy the following files to the <BackupID>\TrapTracker folder

- mymibs.bin
- All files with .ini extension

12. From the <installdir>\WCWindows copy the following folders to the <BackupID>\WCWindows folder

- Policies
- SnapShots
- All files with .ini extension

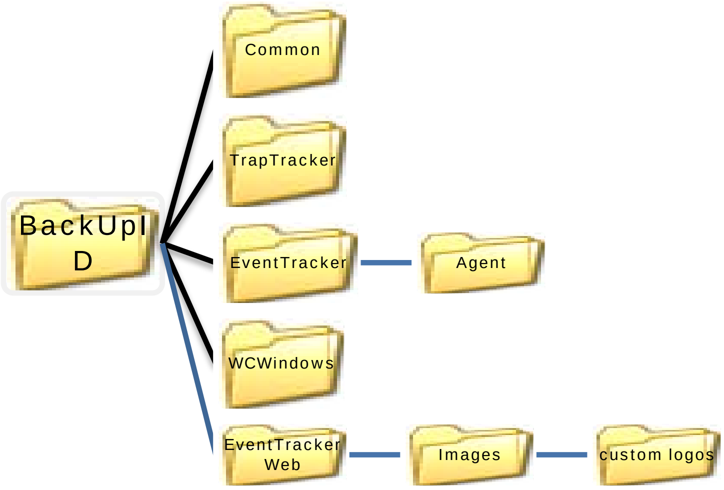
13. Start all the services which were stopped in step 2 and 3.

If the user has used the custom logo,

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



Process of restoration on 'New manager server':

Before you start

- Please ensure that no reports or analysis 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.

Restoring the data on new manager system:

1. 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 is installed)
2. Stop **SQL Express/Server** service.
3. Ensure that all the services mentioned in step 1 & 2 have stopped successfully.
4. Create a folder 'EventTrackerDB' in C:\ drive.
5. Copy the *.mdf and *.ldf files from the <BackupID>\Common folder to 'EventTrackerDB' folder created in step 4.
6. Now you need to replace the files and folders present under <installdir> with those present in <BackupID> of shared medium.

1. 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 .etw extension

2. Copy the following files from the <BackupID>\TrapTracker folder, and replace them under <installdir>\TrapTracker.
    - mymibs.bin
    - All files with .ini extension

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

For users using custom logos,

f. Copy the following folder from the <installdir>\EventTrackerWeb\images\folder and replace them under <BackupID>\EventTrackerWeb\images\folder.CustomLogos

7. Start **SQL Express/Server service**.

8. Rename the ‘Reports’ folder which is copied in step 6.1 to ‘Previous Version Reports’.

9. Run ‘Setpreviousreportpath.bat’ batch file.

10. Run ‘ImportCabReportDetails.bat’ batch file.

11. Run ‘ImportClienttDetails.bat’ batch file. (Should be run on Collection Master)

12. Import all custom Categories, Alerts (Please check the ‘Export E-mail Settings’ check box), Filters, Scheduled Reports and RSS Feeds using Export Import Utility

13. Run the following batch files:

    a. Changearchivepath.bat

    b. Changepreviousgeneratedreportpath.bat

    c. ChangeResultspath.bat

    d. ChangeClientDetailpath.bat (Run on CM when CP’s are reporting)

    NOTE:

    The path needs to be modified in the batch files.

14. Start all the services, which were stopped in step 1.

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

Update all Change Audit agents to point to the new manager

NOTE:

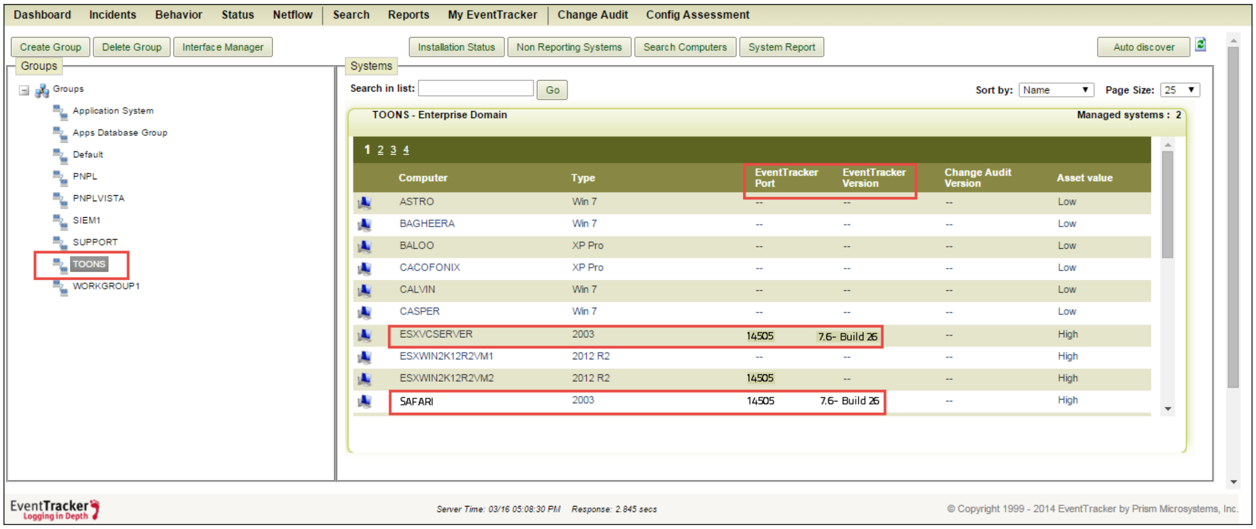
This is applicable only if Change Audit is installed.

Agents which are sending snapshots to existing manager needs to be re-configured to send the snapshots to the new manager.

1. Un-install the all the change audit agents from the existing manager.
2. Install change audit agents from the new manager

Verify the agents status in system manager

Once the new manager is assigned to the agents, then they will become 'managed systems'. The managed system will always display the 'EventTracker version number' and 'EventTracker Port number' in the system manager page.



Sort by: Name ▼ Page Size: 25 ▼

TOONS - Enterprise Domain

Managed systems : 2

1 2 3 4

Computer	Type	EventTracker Port	EventTracker Version	Change Audit Version	Asset value
ASTRO	Win 7	--	--	--	Low
BAGHEERA	Win 7	--	--	--	Low
BALOO	XP Pro	--	--	--	Low
CACOFONIX	XP Pro	--	--	--	Low
CALVIN	Win 7	--	--	--	Low
CASPER	Win 7	--	--	--	Low
ESXVCSERVER	2003	14505	7.6- Build 26	--	High
ESXWIN2K12R2VM1	2012 R2	--	--	--	High
ESXWIN2K12R2VM2	2012 R2	14505	--	--	High
SAFARI	2003	14505	7.6- Build 26	--	High

Server Time: 03/16 05:08:30 PM Response: 2.845 secs

© Copyright 1999 - 2014 EventTracker by Prism Microsystems, Inc.

Figure 10