Netsurion™ | EventTracker

System Transfer Guide

Transferring EventTracker Manager to a new system (v8.2/v8.3 to v9.0)

Publication Date: March 6, 2018

Abstract

Transfer of EventTracker Manager from existing system to new system may be necessitated due to many possible reasons, like 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.

Table of Contents

Instructions for Advanced User

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

1. Install EventTracker 9.0 console on a new system
2. Update all EventTracker Agents/Sensors to point to the new Manager
3. Update all Change Audit Agents/Sensors to point to new Manager
4. Transfer data from the **existing system** to the **new system**
5. Verify the agent status in System Manager

NOTE: Take a backup of any custom configured reports, alerts or filters, behavior rules (not mandatory).

****IMPORTANT:**

1. It is recommended to first migrate the Collection Master and then migrate the Collection point.
2. Please apply all the updates in proper order for v8.2/v8.3, before proceeding with the migration.

Common steps for all console types:

Install the EventTracker manager on a new system

Settings for the 'New manager' system:

NOTE: User should be a Sys Admin for the SQL.

I. Install EventTracker v9.0 in a new system by selecting appropriate Console type. For detailed installation instructions, please refer EventTracker Installation Guide for respective versions.

NOTE: After successful migration from (v8.x to v9.0), please apply all the v9.0 updates in appropriate order.

II. Reconfigure the EventTracker Agents\Sensors and ChangeAudit agents\sensors to the New manager system. To do this, please follow the sections: "**Update all EventTracker agents to point to the new manager**" and "**Update all Change Audit agents to point to the new manager**".

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)

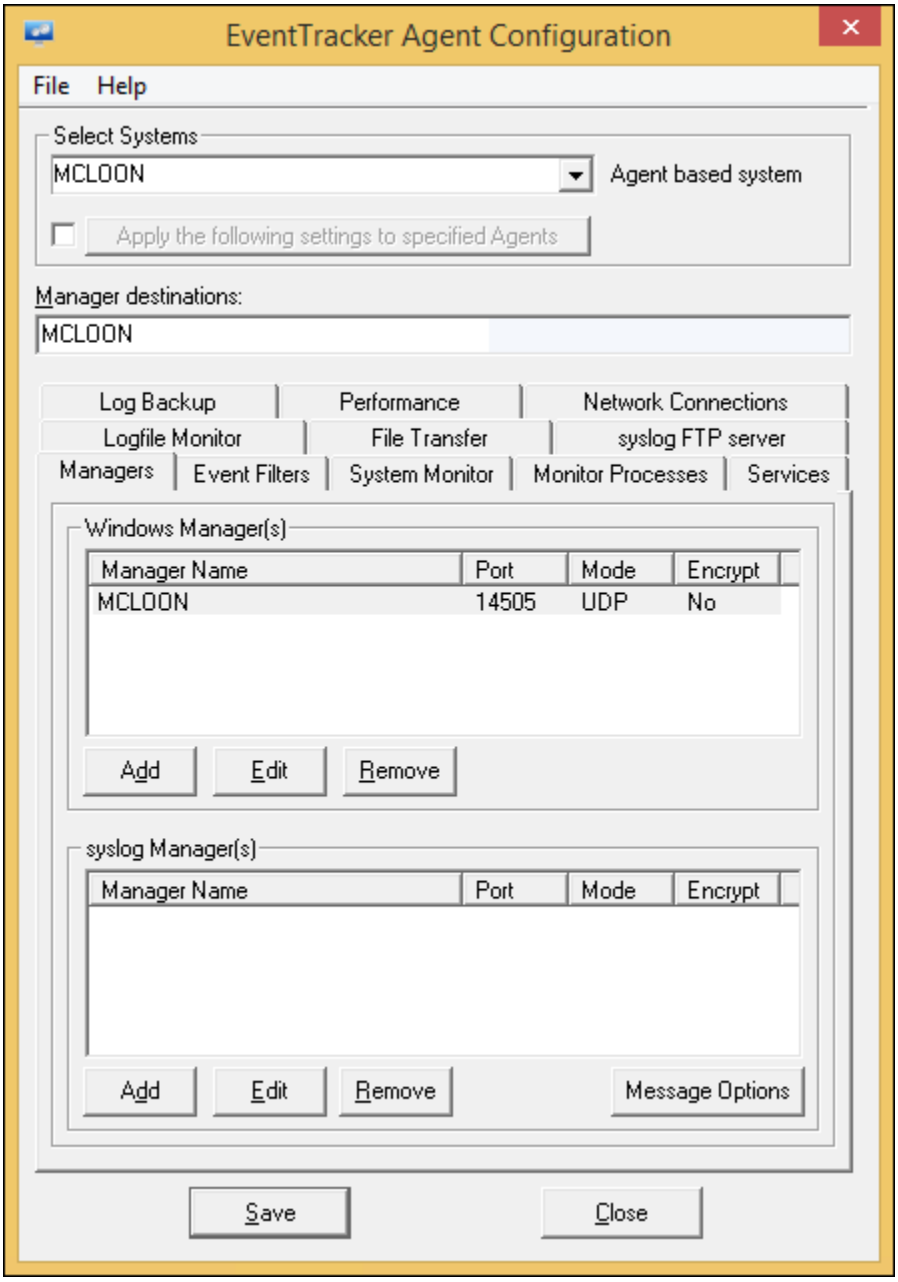


Figure 1

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

   For example: SAFARI

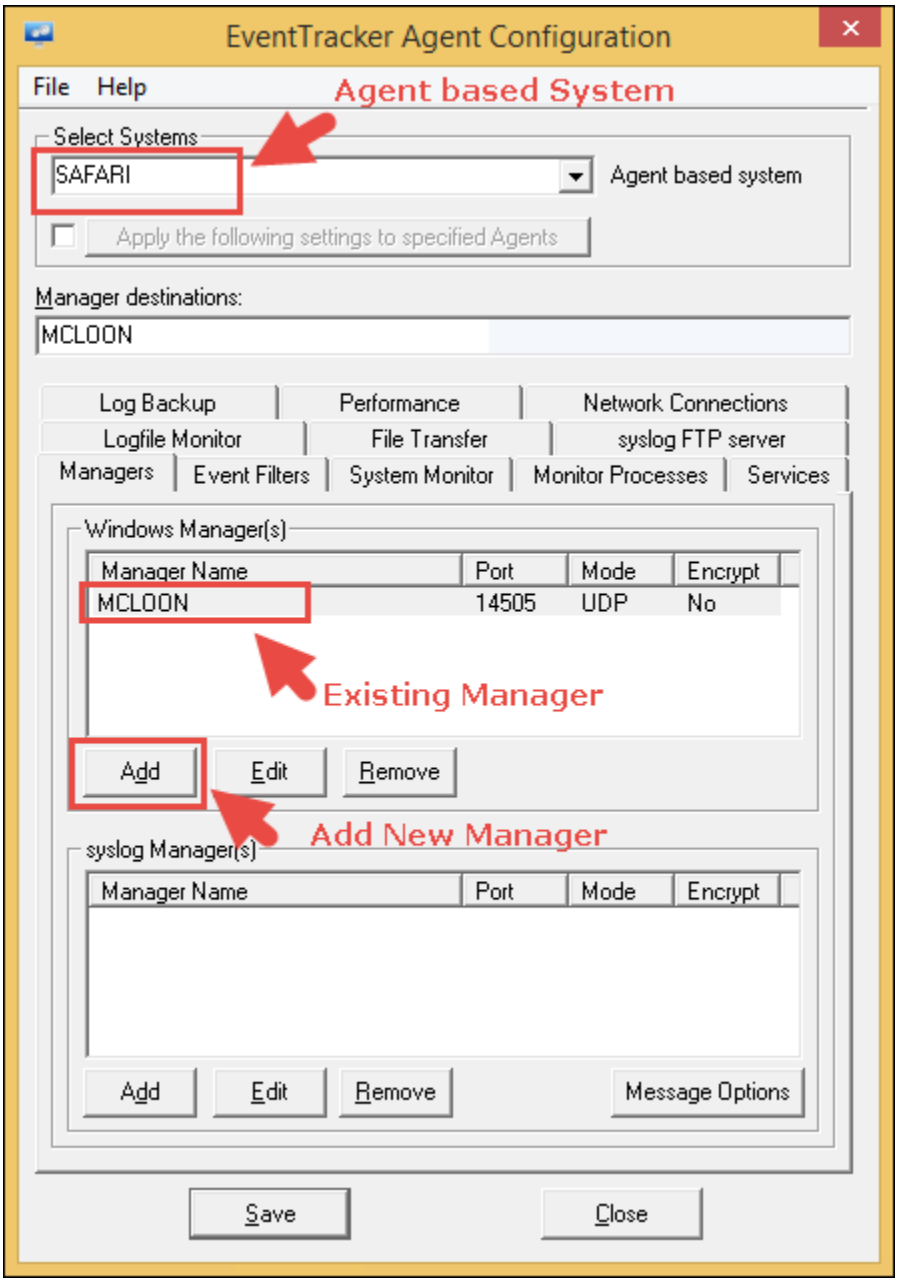


Figure 2

3. Click the **Add** button.

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

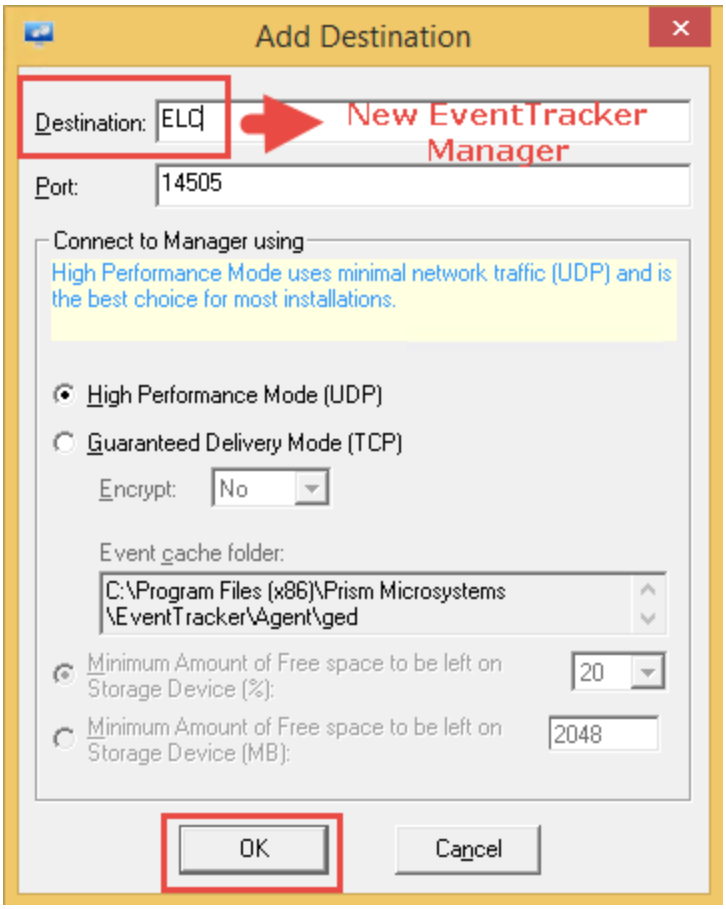


Figure 3: Add Destination

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.

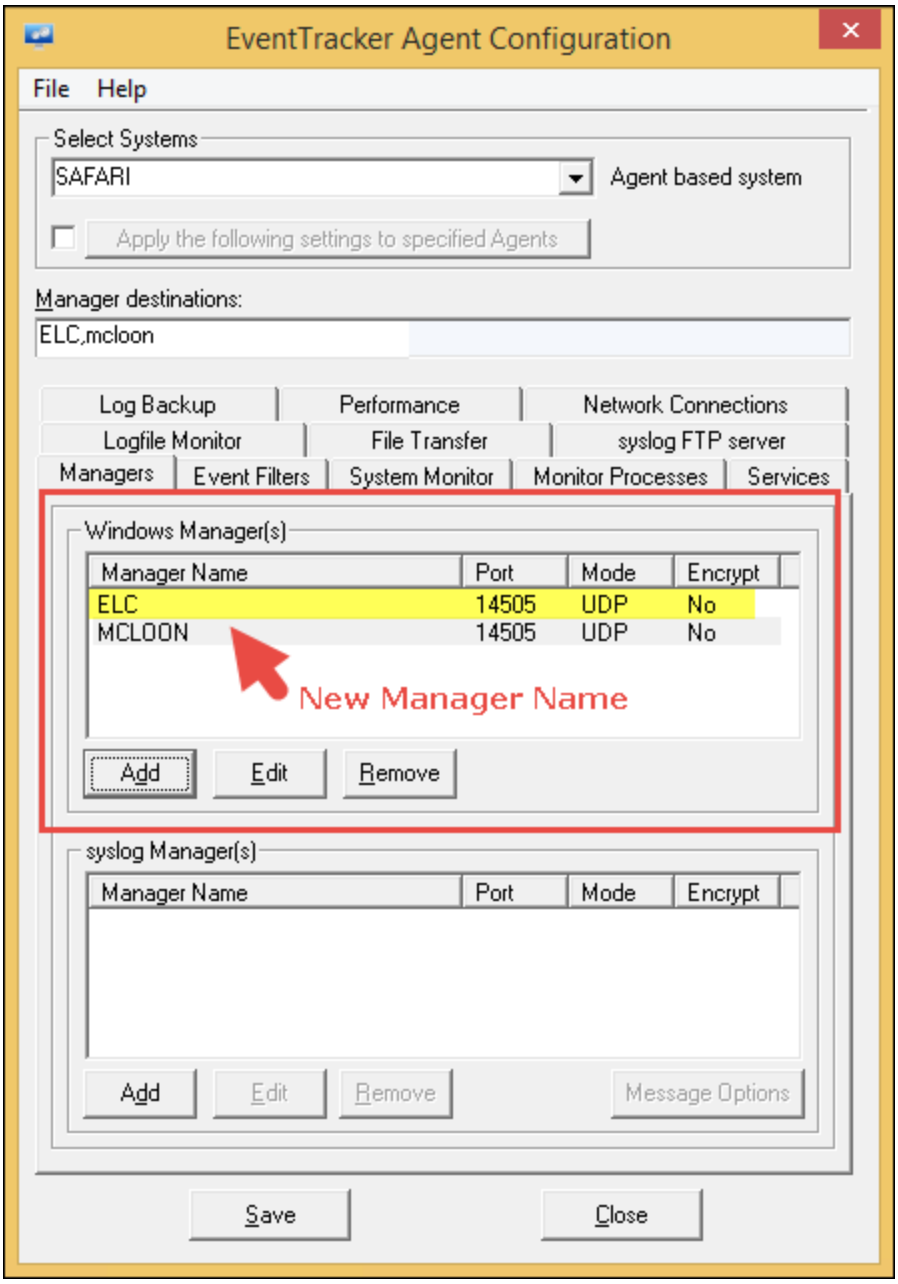


Figure 4

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.

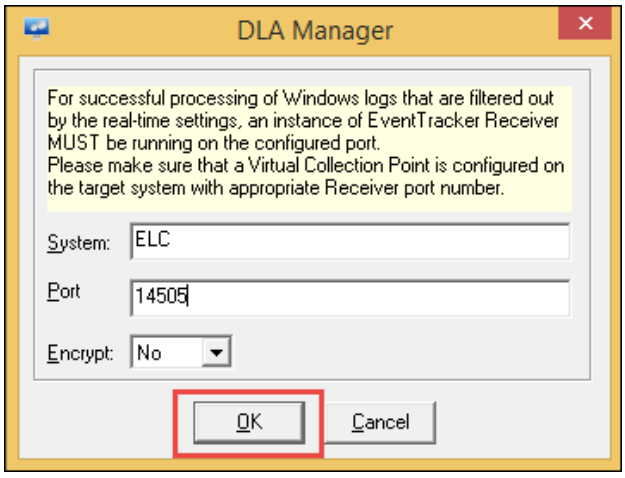


Figure 5

10. Click the **OK** button.

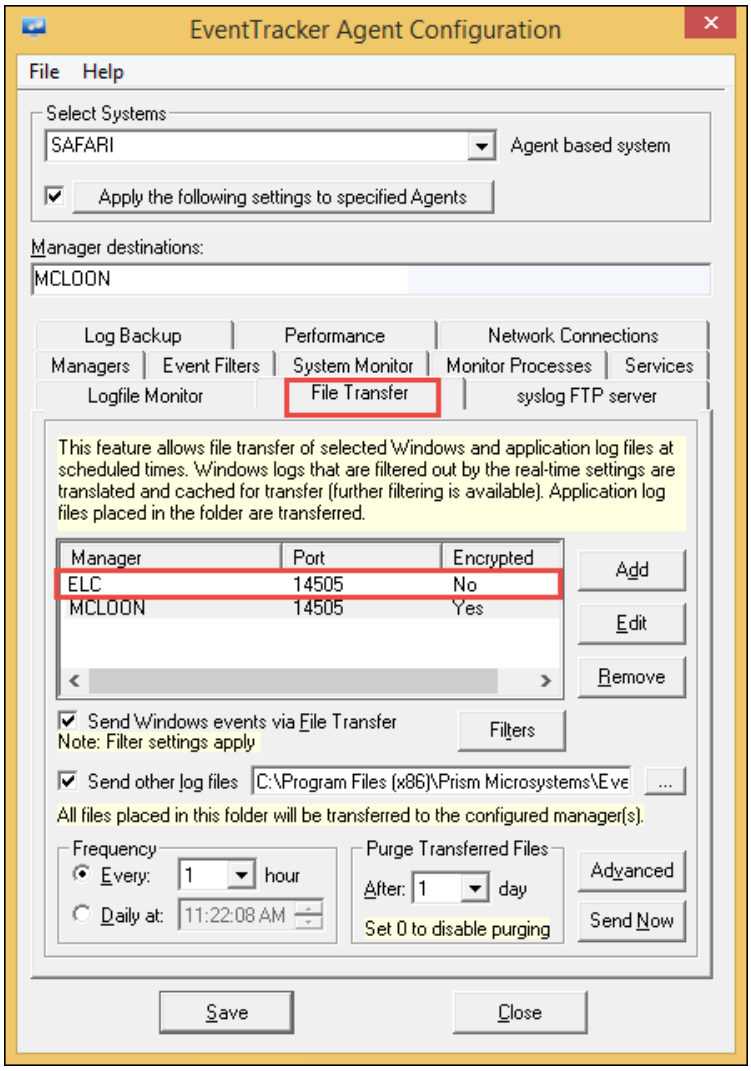


Figure 6

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

    EventTracker removes the existing manager name from the list.

    NOTE:

    After migration is complete, the user can delete or retain the old manager name.

12. Now, from **File** dropdown, select the **License Server**.

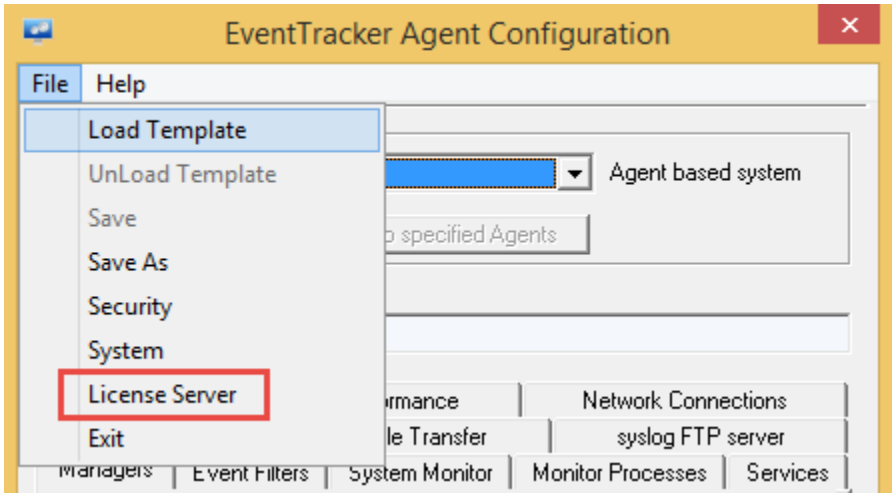


Figure 7

13. Update the License Server with the New Manager name, and then click on **OK**.

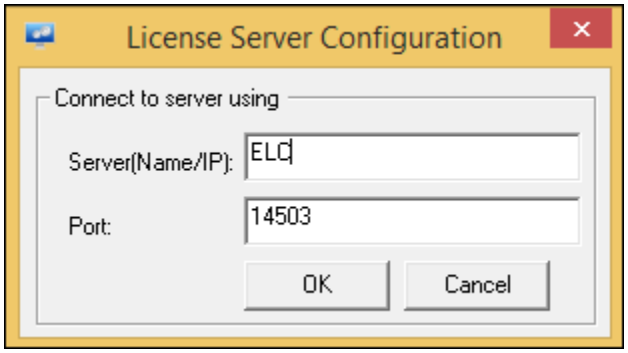


Figure 8

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

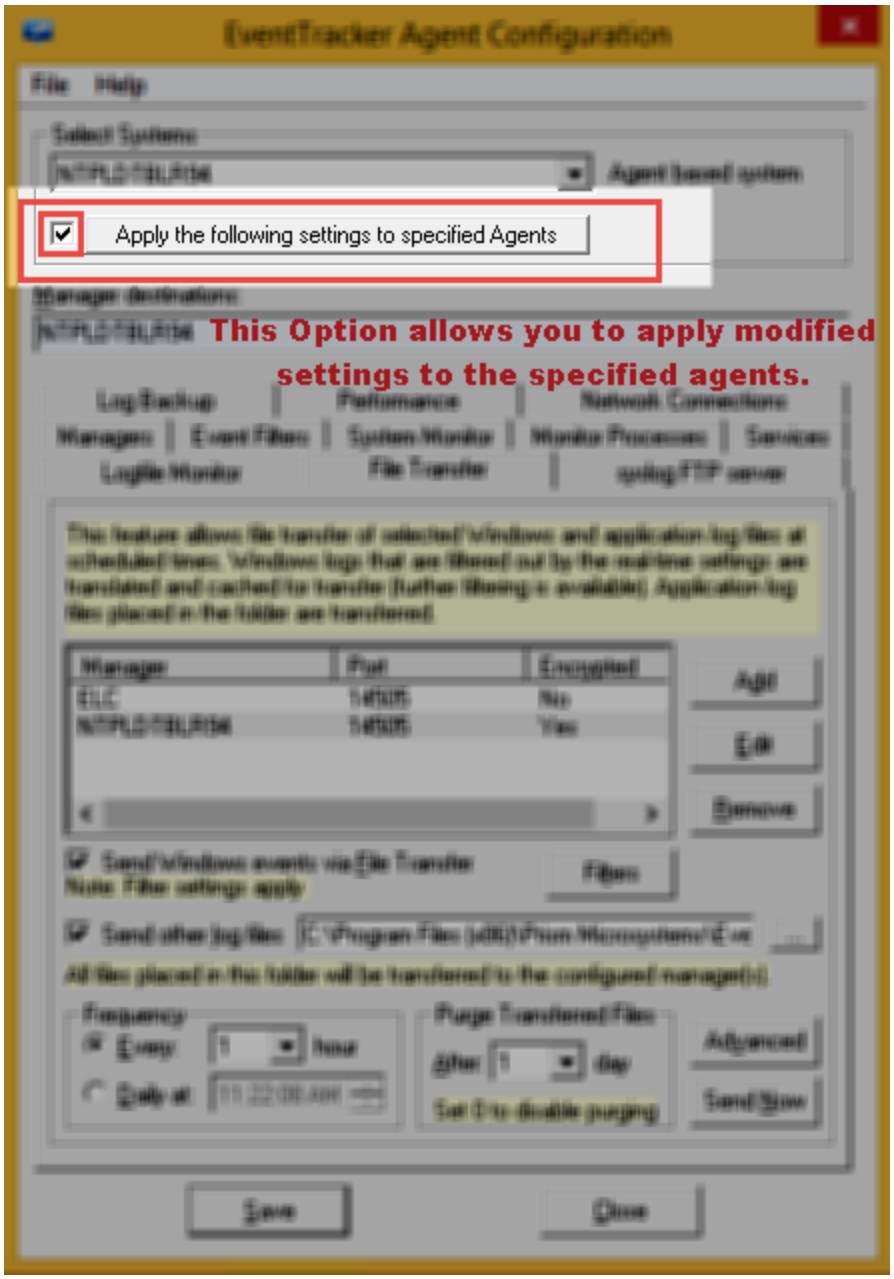


Figure 9

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

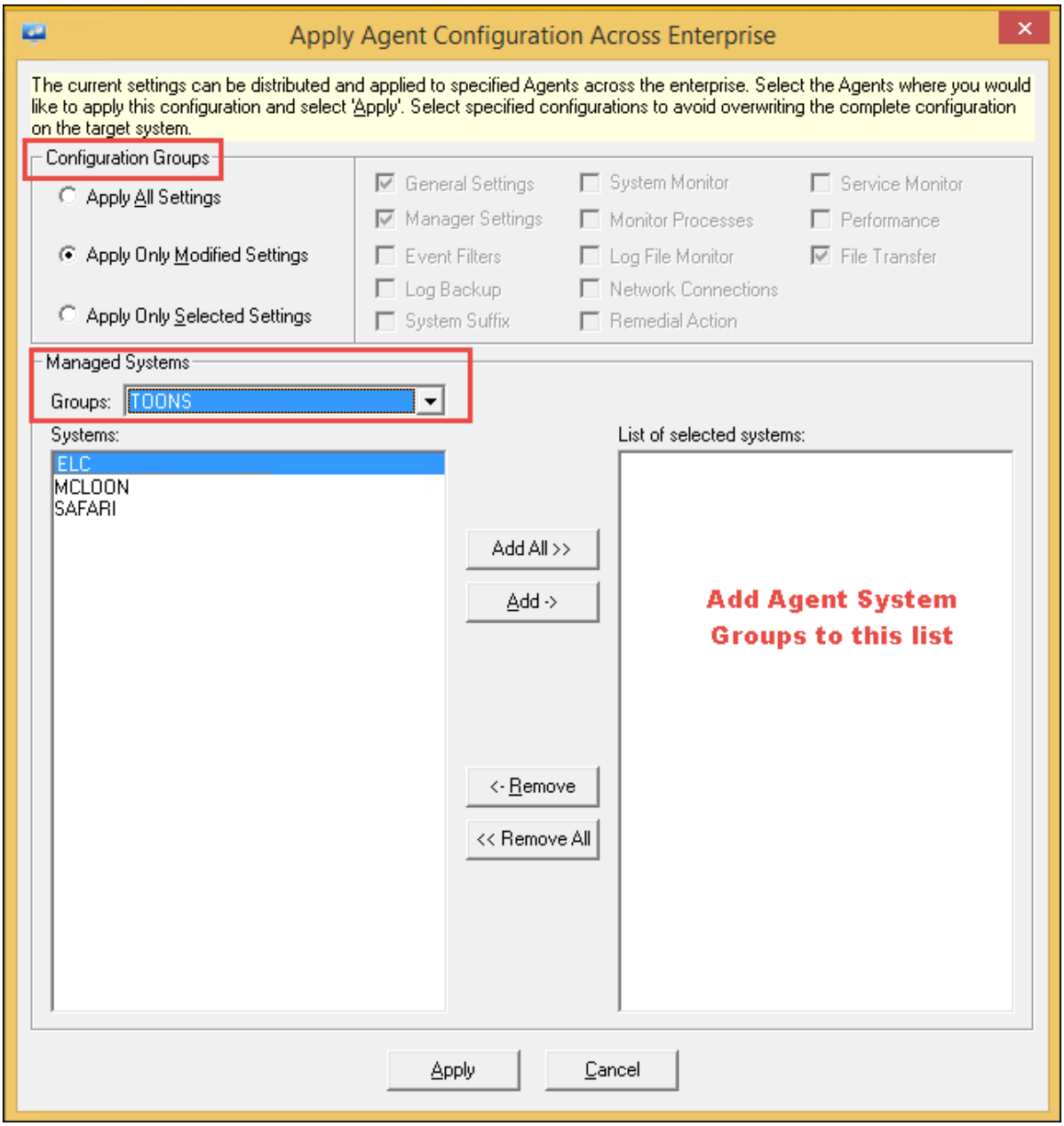


Figure 10: Apply Agent Configuration Across Enterprise

16. 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.

17. From the **Groups** dropdown, select the group name where the agent systems are present.
18. 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**
19. Click the **Apply** button.

EventTracker displays a warning message. (Refer Figure 7)

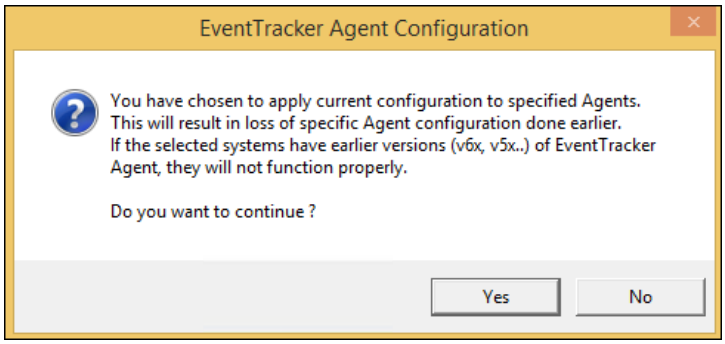


Figure 11

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

NOTE: For the non-windows devices such as firewall, router, switches, etc., change the forwarding IP address to the new EventTracker Manager console IP Address.

Update all Change Audit agents to point to the new manager

The below mentioned steps are to be performed in an Old Manager (v8.2/v8.3).

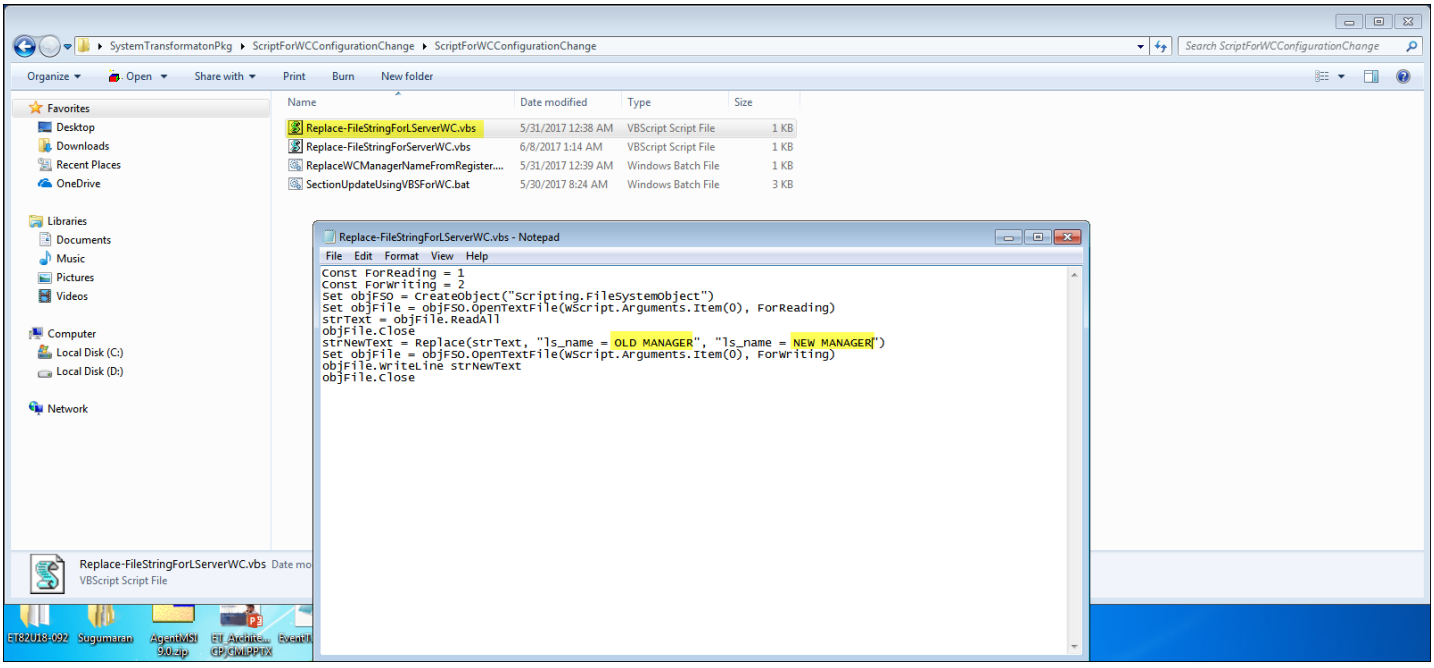
Download the package from the below link:

https://sharepoint.eventtracker.com/prism/SystemTransformationPackage

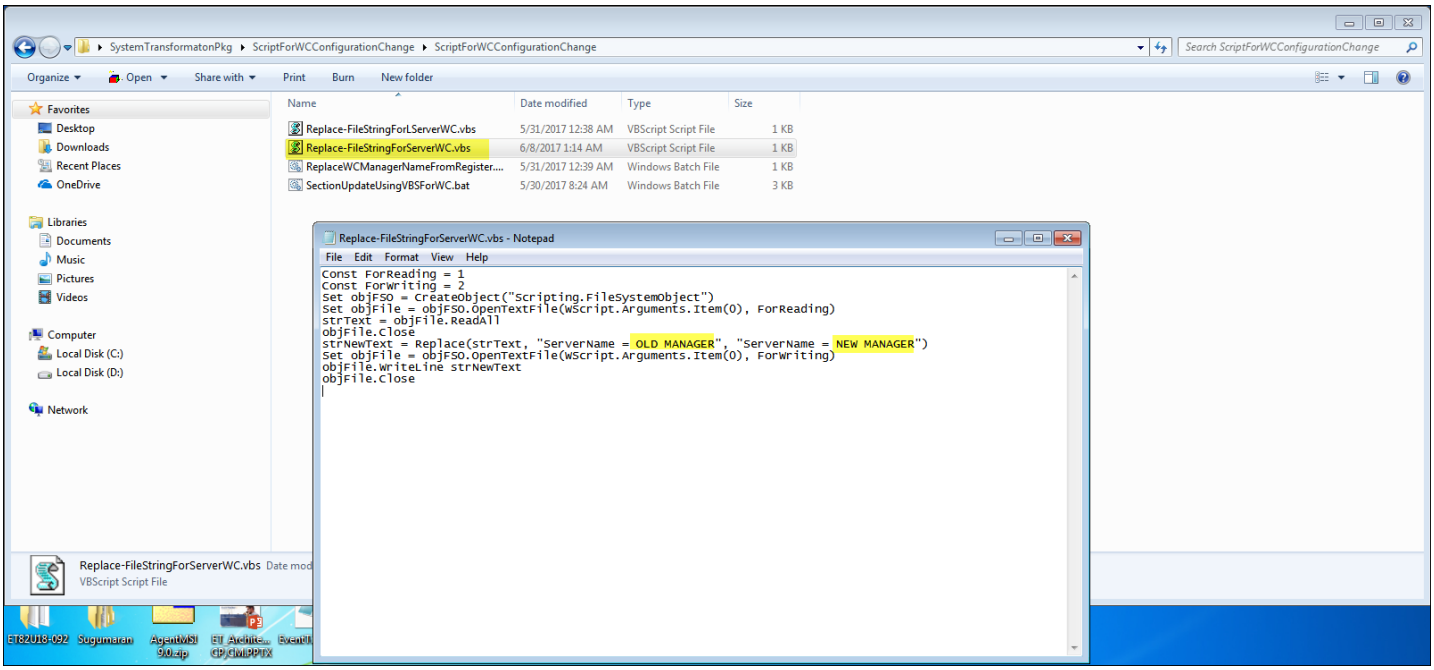
Open the folder "**ScriptForWCConfigurationChange**".

\ScriptForWCConfigurationChange\ScriptForWCConfigurationChange

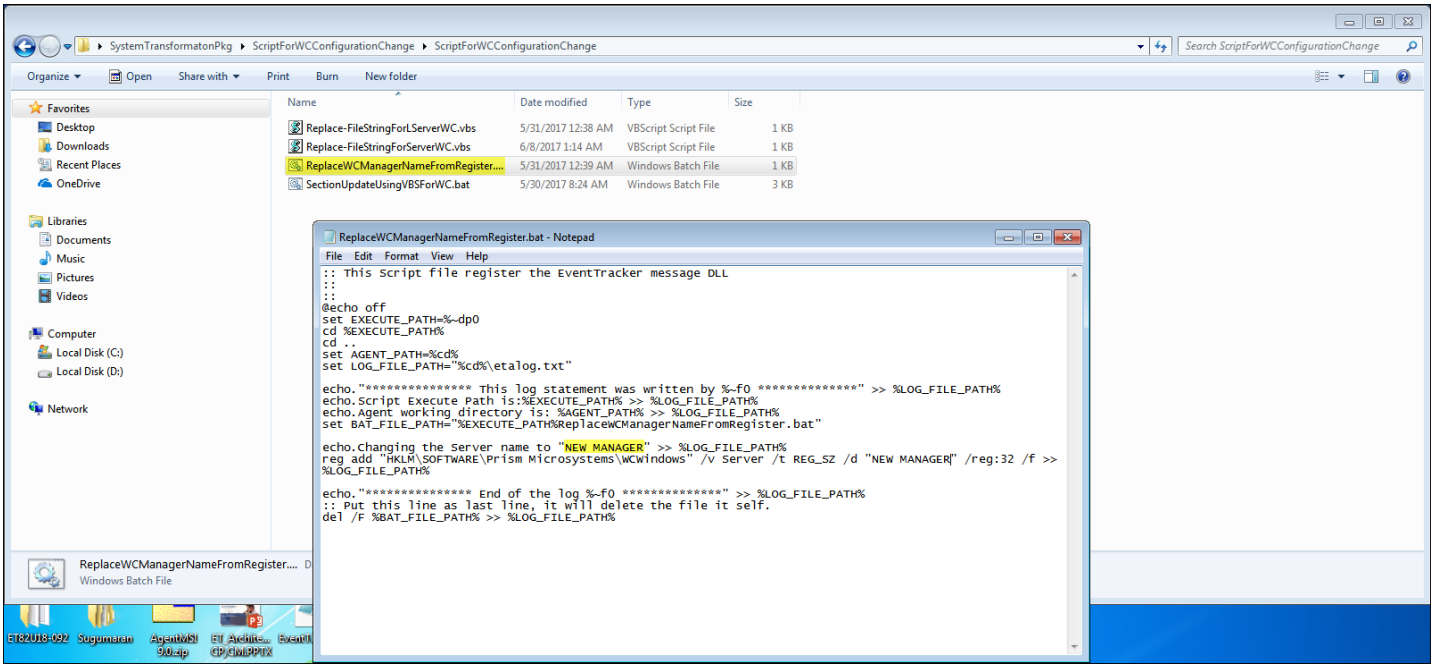
- In the script files, in place of "Old Manager" type the v8.2/v8.3 Manager name. In place of "New Manager" type the 9.0 Manager name.



Replace-FileStringForLServerWC.vbs



Replace-FileStraingForServerWC.vbs



ReplaceWCManagerNameRegister.bat

- Make the above changes in the files and save it.
- Now, open the ….install directory\EventTracker\Agent and run the "**etaDataDispatcher**" as an administrator.

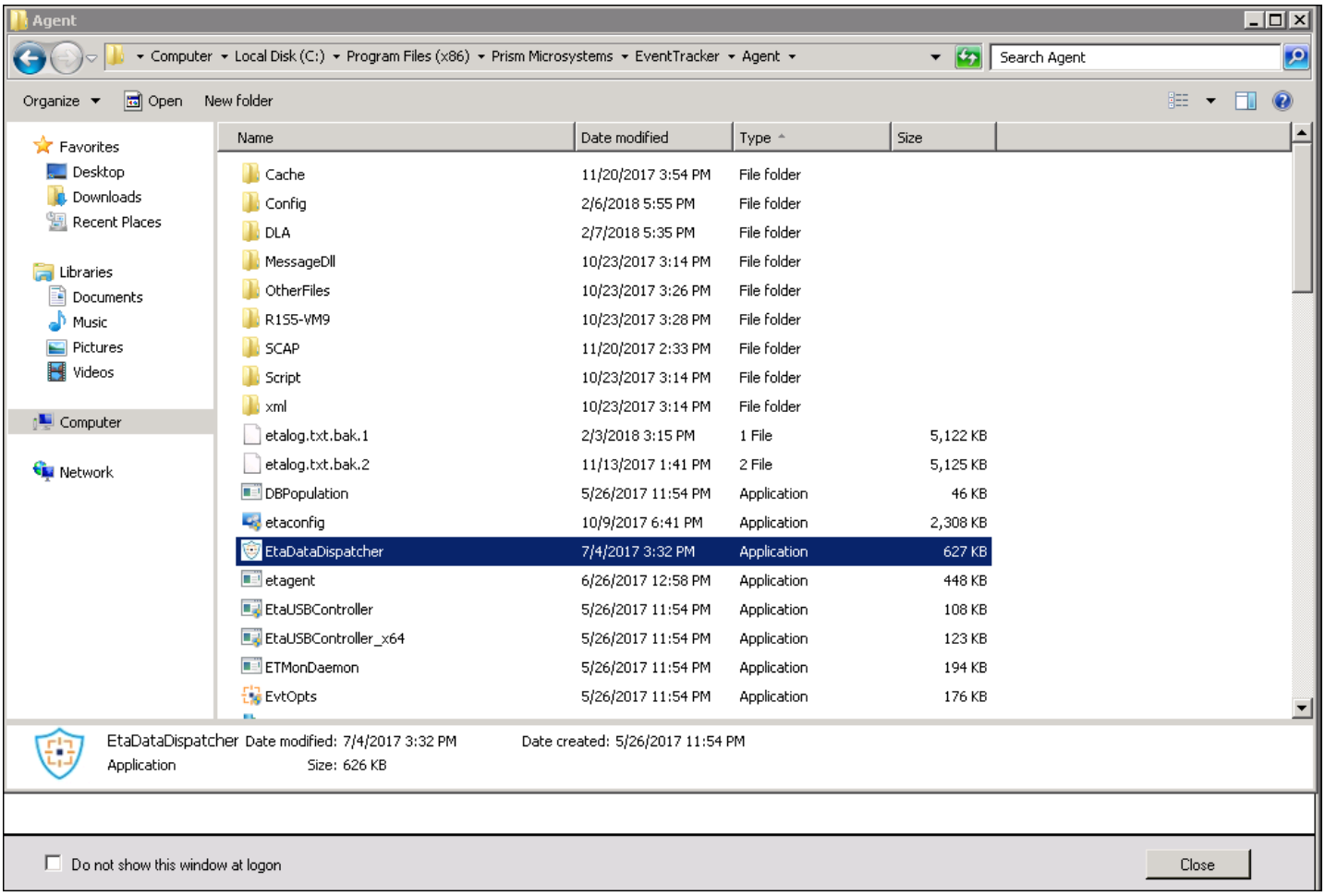


Figure 12

- Check the "**Send Script Data**" and "**Send Executive Script**" option.

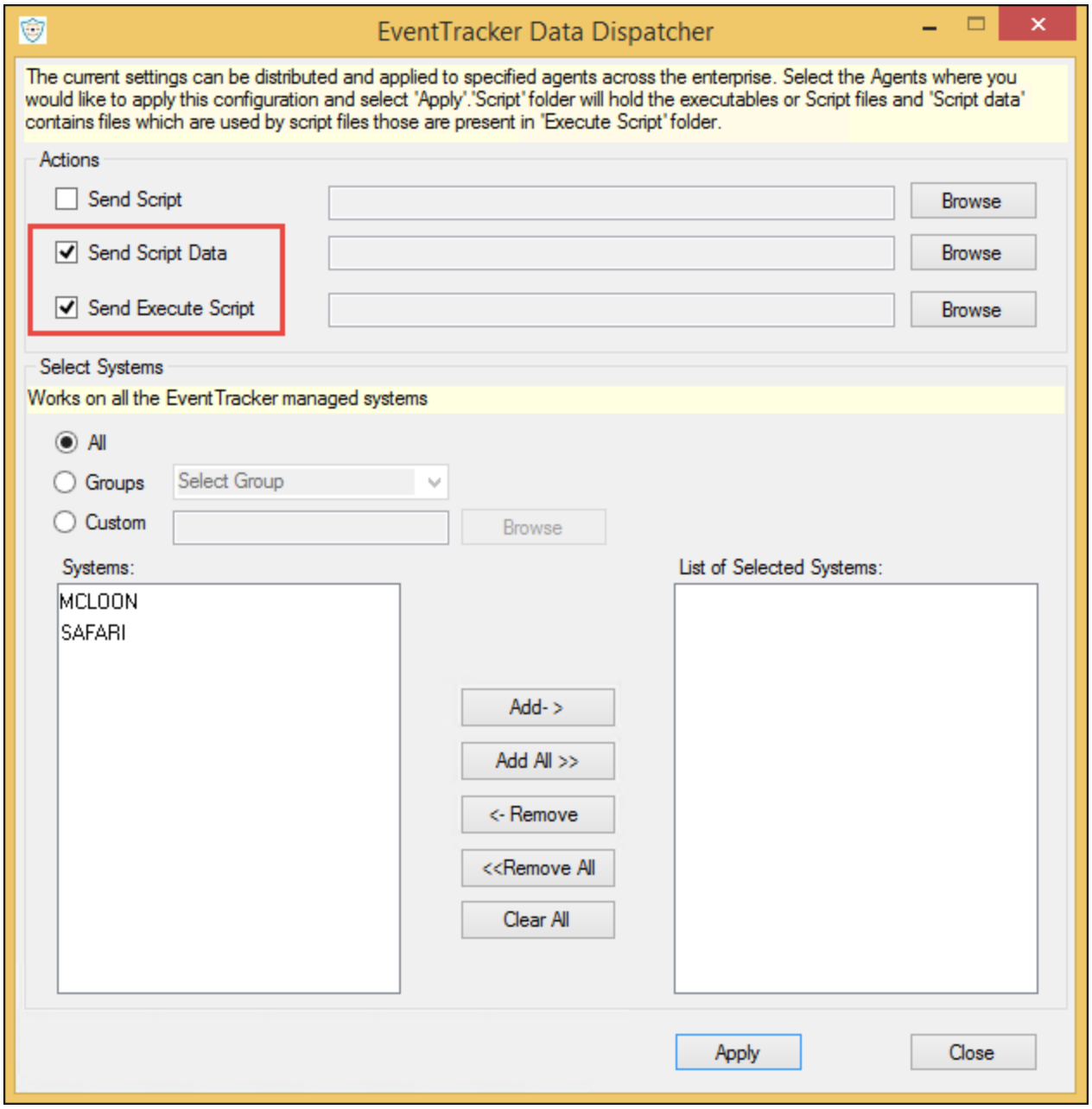


Figure 13

- For " **Send Script Data**" option, browse the script files (vb script files)and select the ones shown in the below figure:

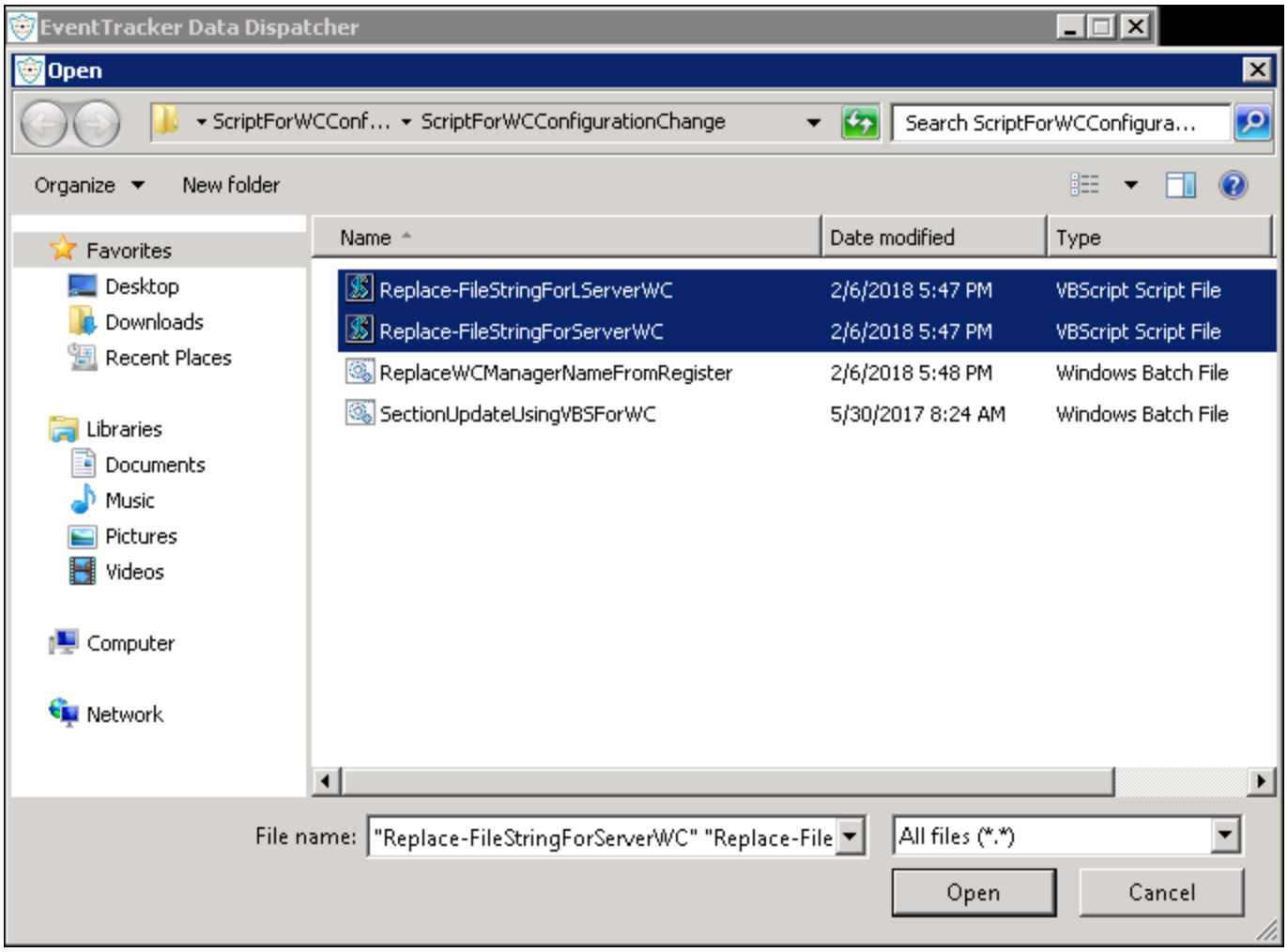


Figure 14

- For "**Send Execute Script**", browse and select the batch files i.e. "**ReplaceWCManagerNameFromRegister**" and "**SectionUpdateUsingVBSForWC**".

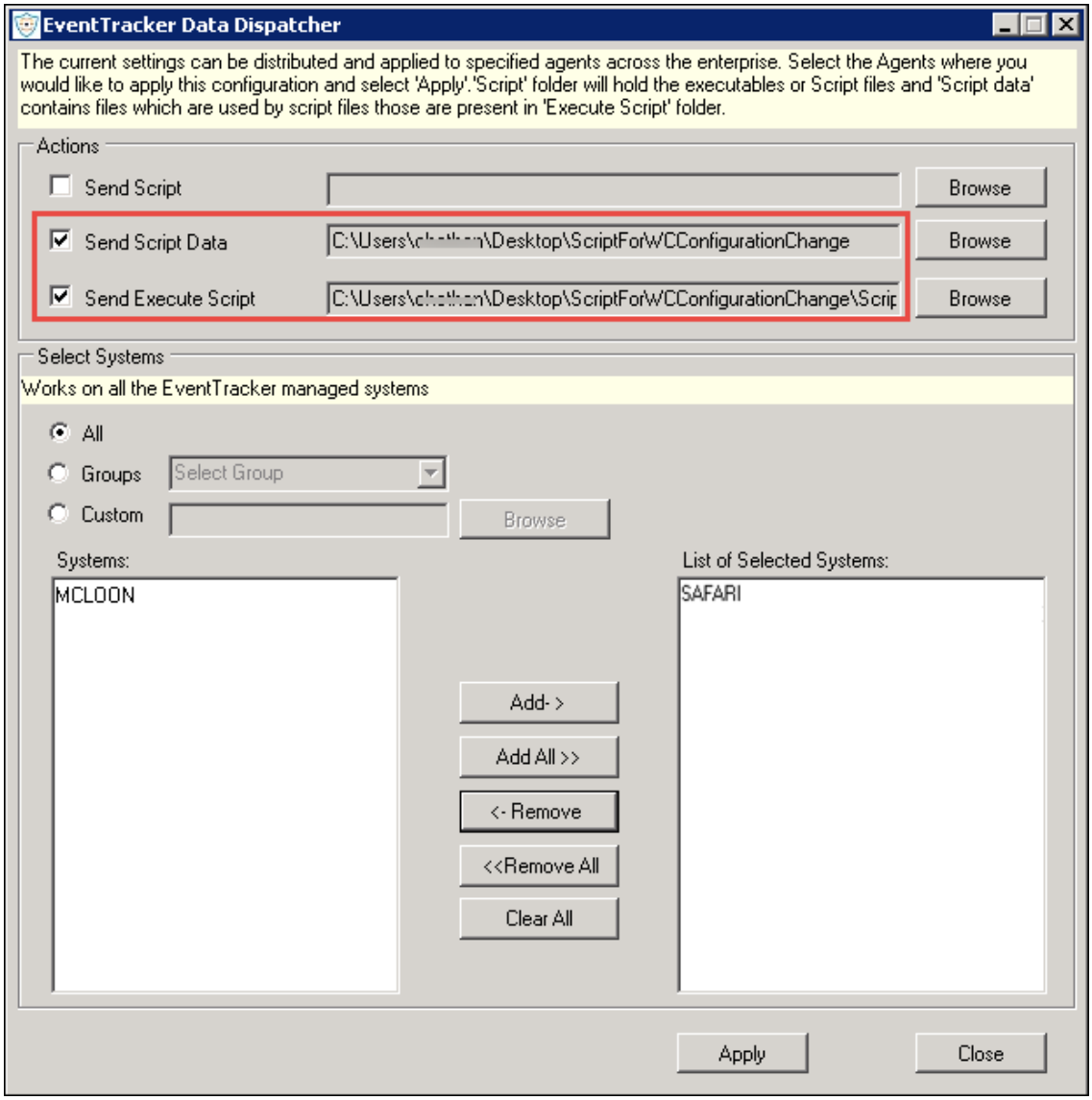


Figure 15

- Click on **Apply** and a success message gets displayed.

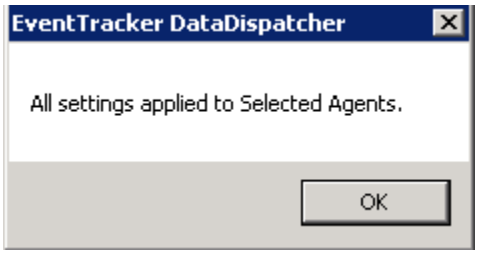


Figure 16

III. Ensure that no reports 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 in v8.2/v8.3.

IV. Verify the processes and make sure that '**Prism.Reports.ServiceProcessor.exe**' is not running in v8.2/v8.3.

V. After forwarding all the agents Stop\Disable all the EventTracker services including SQL in both environments (v8.2/v8.3 and 9.0).

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

- EventTracker Daemon
- EventTracker Agent
- EventTracker Scheduler
- EventTracker Alerter
- EventTracker EventVault
- EventTracker Indexer
- EventTracker Receiver
- EventTracker Remoting
- EventTracker Reporter
- EventTracker WatchList
- EventTracker Elasticsearch Indexer(applicable for 9.0)
- elasticsearch-service-x64(applicable for 9.0)
- WcwService (If Change Audit is installed)
- TrapTracker Receiver (If TrapTracker is installed)
- Event Correlator (If Correlator update is installed)

VI. Before copying the EventTracker v8.2/v8.3 configuration files, cut the archives folder of EventTracker v9.0 and keep it as a backup.

VII. In the EventTracker 9.0 Environment, create a folder named "**EventTrackerV9**" in C drive.

VIII. Copy the following files from install path of EventTracker 9.0 which is in the common folder and paste the copied files to the path "**C:\EventTrackerV9**"

a. EventTracker.mdf

b. EventTracker_log.LDF

c. EventTrackerAlerts.mdf

d. EventTrackerAlerts_log.LDF

e. EventTrackerData.mdf

f. EventTrackerData_log.LDF

IX. Share the Archive path of EventTracker v8.2/v8.3 (old machine). It should be accessed from 9.0 (New machine).

X. Create folders named Common, EventTracker,TrapTracker and WcWindows in the Backup folder which is in shared path by copying it from v8.2/v8.3.

Go to the <installdir>\Common folder.<Installdir> is the full path of the directory where EventTracker is installed.

a) From the above folder copy the *.mdf and *.ldf files, and store them in the newly created Common sub folder under the Backup folder. (**SiteDB needs to be copied, if it is a v8.2/v8.3 Collection Master**)

XI. Create a Backup folder in a shared path where EventTracker 9.0 machine can access.

1. From the <installdir>\EventTracker, copy the following folders/files to the Backup folder.

- Reports
- Cache
- AgentConfig
- All the files with .etw extension

For users who are having the TrapTracker feature,

2. From the <installdir>\TrapTracker copy the following files to the Backup\TrapTracker folder

- mymibs.bin
- All files with .ini extension

For users who are having the Change Audit feature,

3. From the <installdir>\WCWindows copy the following folders to the Backup\WCWindows folder

- Policies
- SnapShots
- All files with .ini extension

If the user has used the custom profile,

4. Create a sub folder named EventTrackerWeb\images\People under Backup folder and copy the People folder to Backup\EventTrackerWeb\images\People\

5. Paste all the files and folders from backup of v8.2/v8.3 to 9.0 machine to the respective folders as mentioned below:

b) Copy the *.mdf and *.ldf files from the EventTracker v8.2/v8.3 backup in the shared path Backup\Common and replace it in the --%InstallDir%\\Common\ folder. (**SiteDB needs to be copied, if it is a v8.2/v8.3 Collection Master**)

c) Copy the following folders from the Backup\EventTracker folder, and replace them under installdir\EventTracker.

- ✓ Archives (Note: Replace the shared Archives of v8.2/v8.3 to the Archive path configured in the new environment)
- ✓ Reports
- ✓ Cache
- ✓ AgentConfig
- ✓ All the files with .etw extension

d) For users who are having TrapTracker feature they can copy the following files from the Backup\TrapTracker folder, and replace them under <installdir>\TrapTracker.

- ✓ mymibs.bin
- ✓ All files with .ini extension

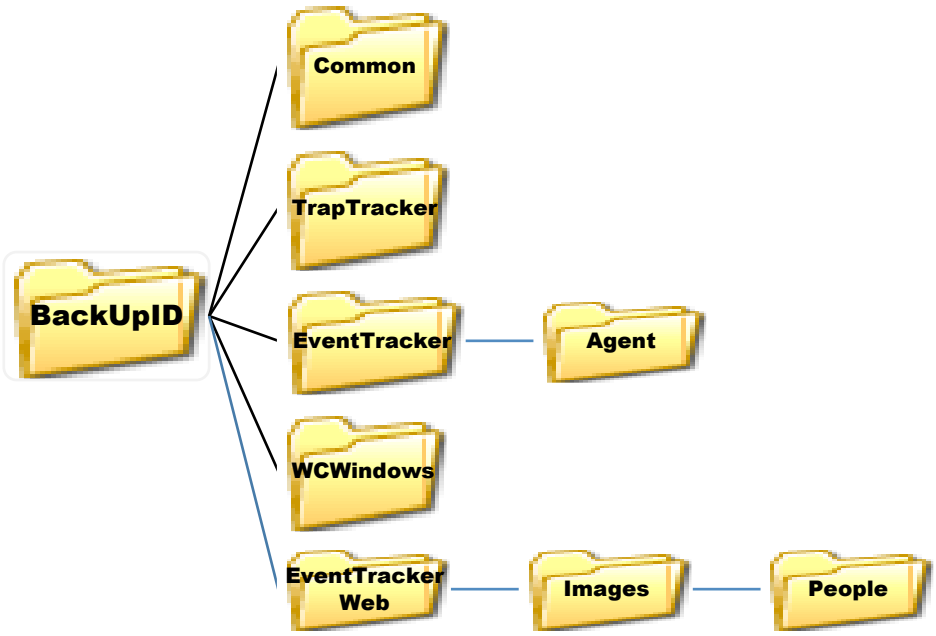
e) For users who are having Change Audit feature they can copy the following folders from the Backup\WCWindows folder and replace them under <installdir>\WCWindows.

- ✓ Policies
- ✓ SnapShots

- ✓ All files with .ini extension

For users using custom profile,

6. Copy the following folder from the Backup\EventTrackerWeb\images\People folder and replace them under <installdir>\EventTrackerWeb\images\People



Standard console Migration:

1. Follow the steps mentioned in the "Common to all Console Types" section.
2. Download the package from the below link: https://sharepoint.eventtracker.com/prism/SystemTransformationPackage
3. Open the folder "**SystemTransformationPkg**"

   \SystemTransformationPkg\SystemTransformatonPkg

4. Start the SQL Service in EventTracker 9.0
5. Before running the batch file, update the SQL Server instance in- **UpdateArchivePath_tbl_config.bat** as shown in the figure below:

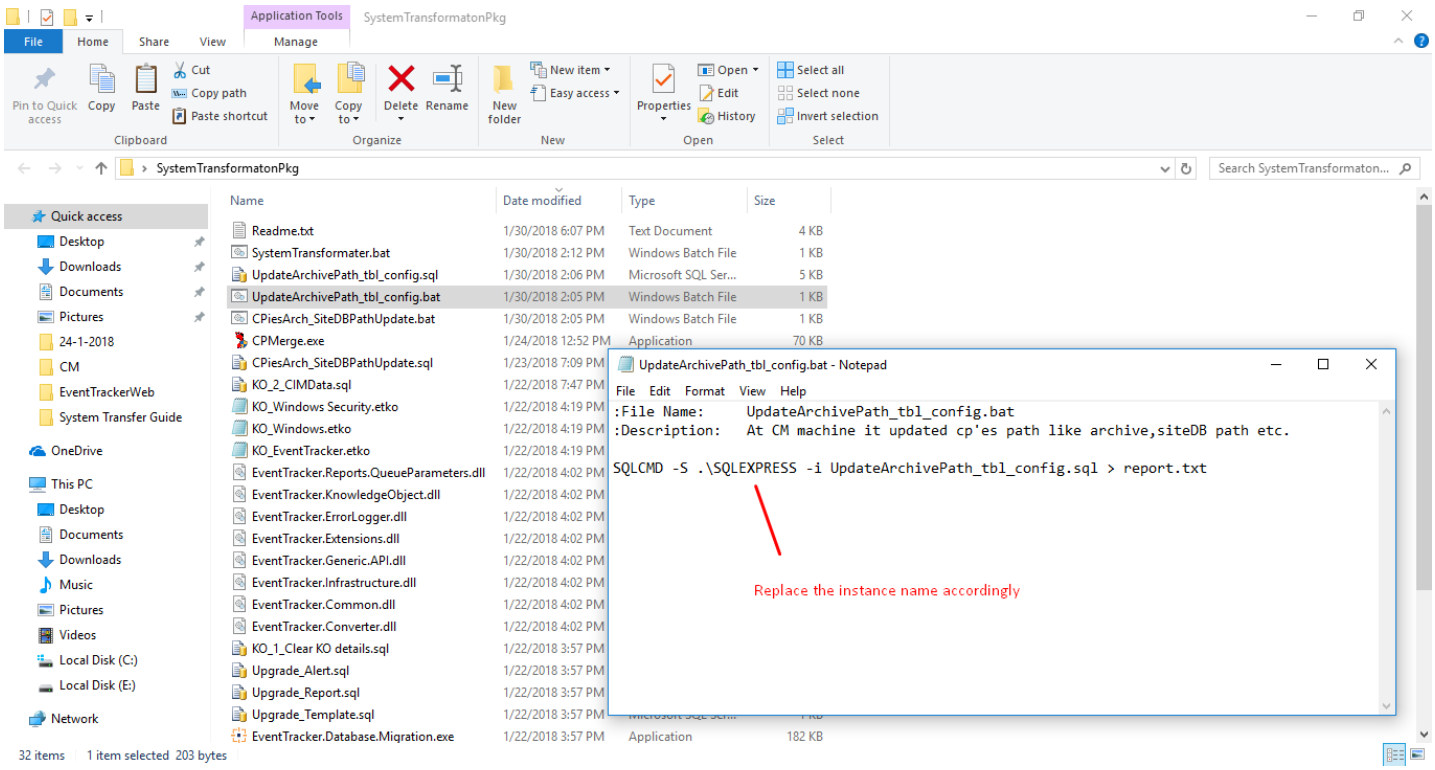


Figure 17

The SQL instance can be taken from the registry path "**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Prism Microsystems\EventTracker\Manager**" from the SQLINSTANCENAME key

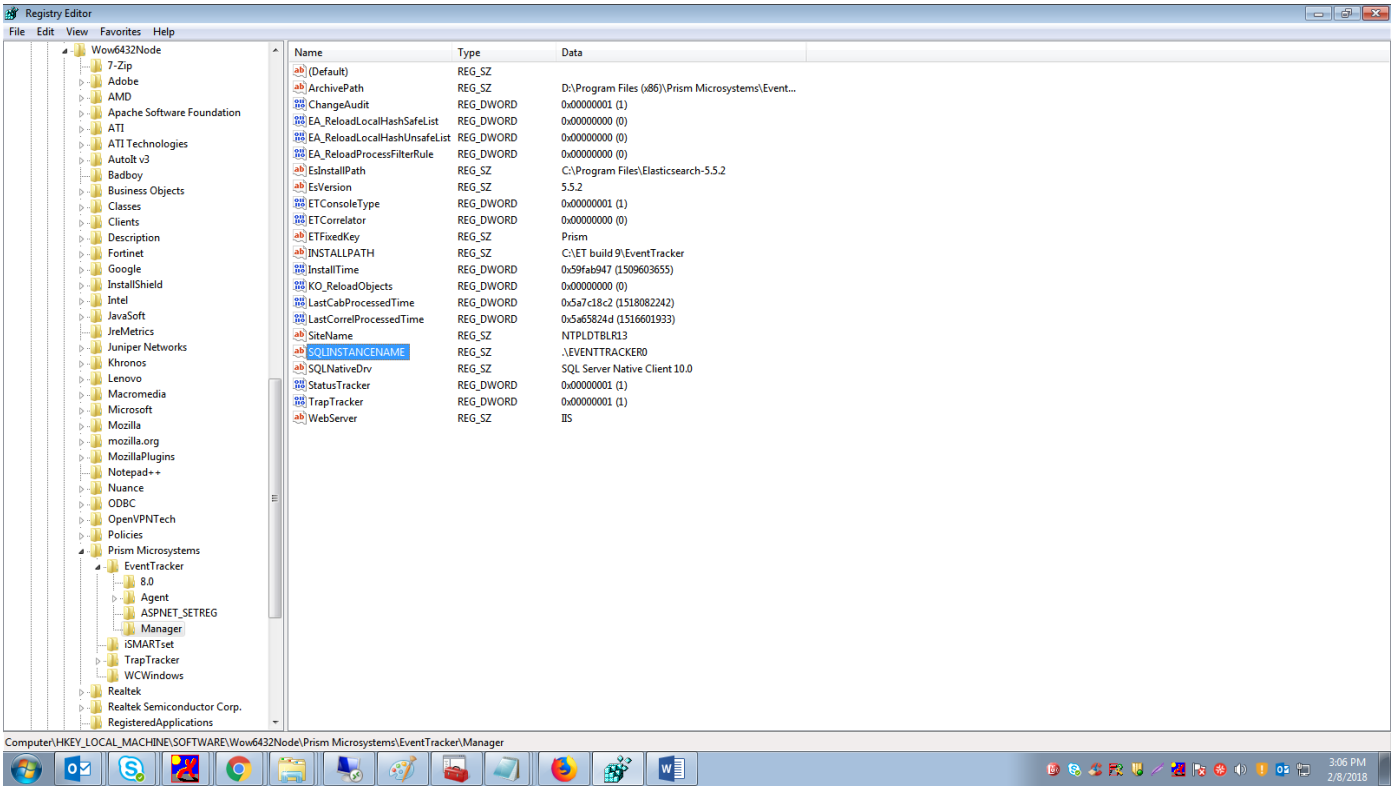


Figure 18

6. Run the following batch files kept in the "**SystemTransformationPkg**" with admin privileges.

   - -Run "**SystemTransformater.bat**" and wait for completion.
   - -Run "**UpdateArchivePath_tbl_config.bat**" and wait for completion.

7. Now start all EventTracker services.

Collection Point Console (CP) Migration:

1. Follow the steps mentioned in the "Common to all Console Types" section.
   The steps for CP Migration are the same as the "Standard Console".

   NOTE: After the migration is completed, the user can append the archives using Append Archives in EventTracker Control Panel.

Collection Master Console (CM) Migration:

1. Follow the steps mentioned in the "Common to all Console Types" section.
   The steps for CM Migration are the same as the "Standard Console".

2. After following the above steps, Attach the CP Site Databases manually to the SQL from the Common folder of EventTracker install directory. (<InstallDir>\PrismMicrosystems\Common\Sites_DB\CP_SITENAME\Common).

3. -Run " **CPiesArch_SiteDBPathUpdate.bat**" and wait for completion.

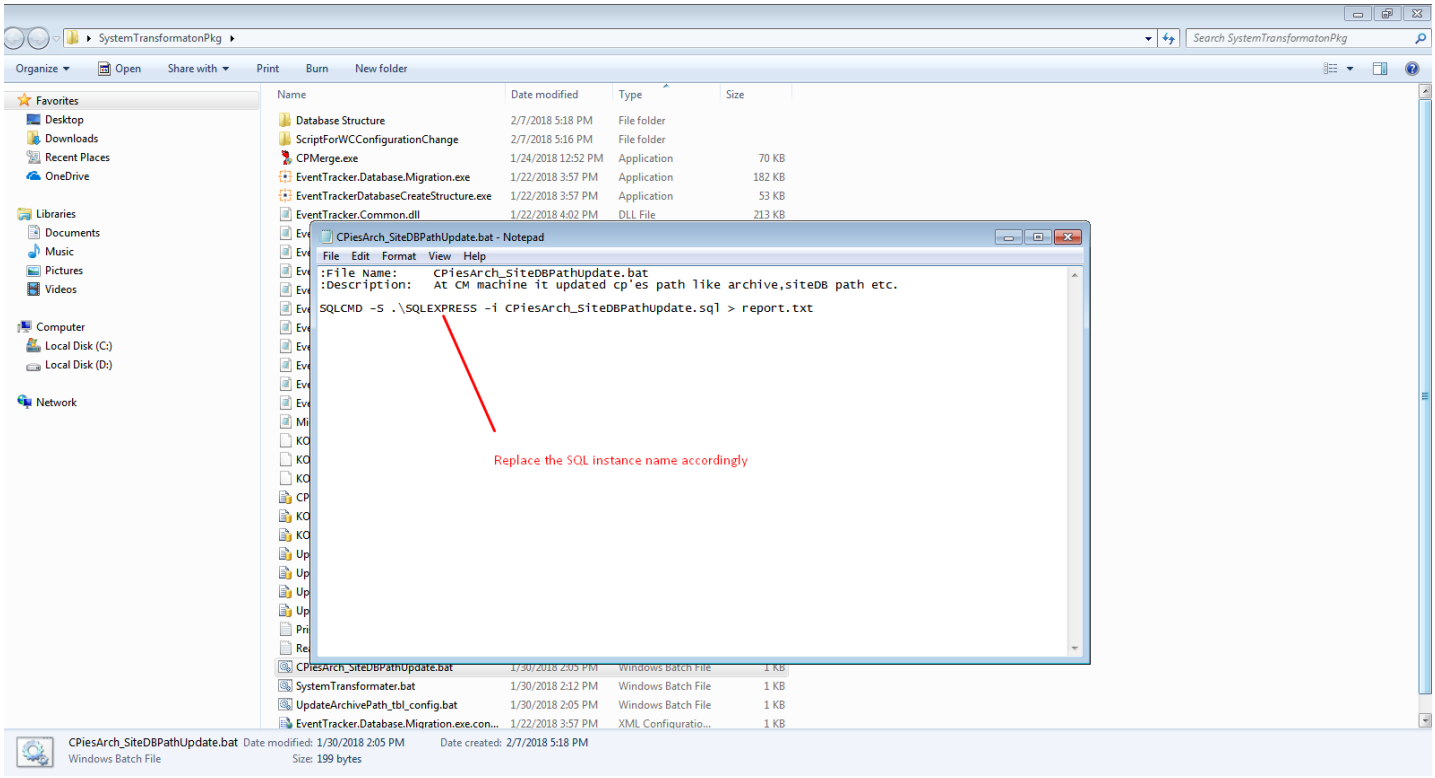


Figure 19

Collection Point (CP) merging in Collection Master (CM)

As the 8.2/8.3 CM gets dismantled, and the 8.2/8.3 CPs as well as the 9.0 CPs starts reporting to the 9.0 CM, it becomes important to merge the 8.2/8.3 CPs to 9.0 CPs.

In our example, we are merging an older v8.2/v8.3 CP (NTPLDTBLR103) to v9.0 CP i.e. (R1S5-VM3).

In the EventTracker Database, it will list both the CPs before merging. This is shown below:

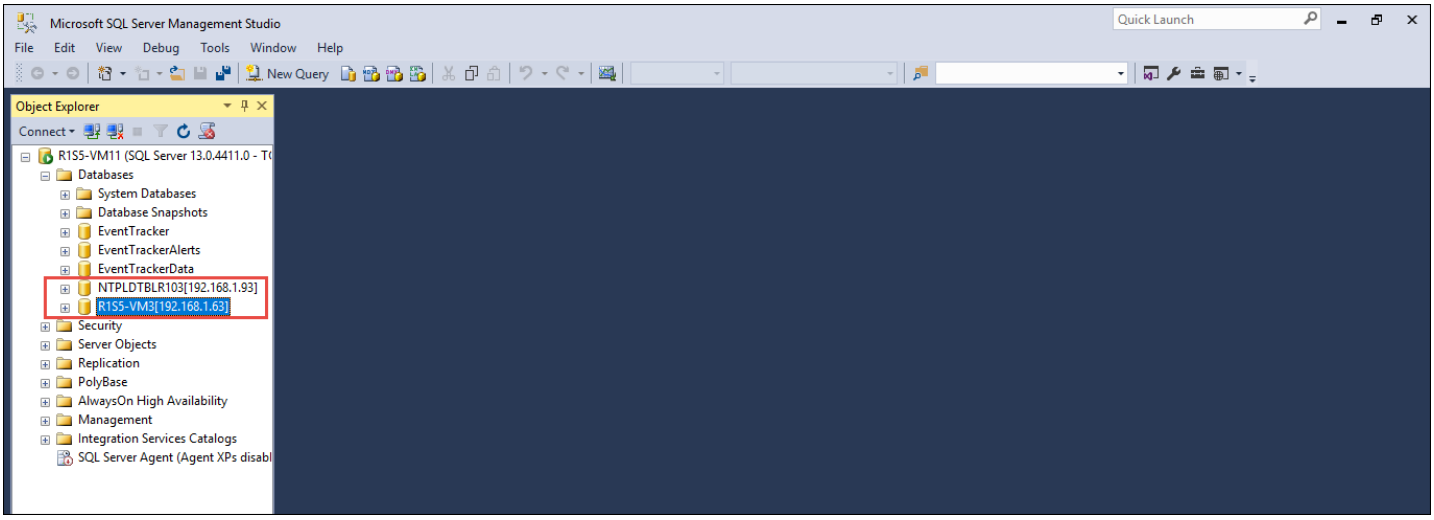


Figure 20

To merge the CPs,

1. Download the package from the site.
2. Copy the package "**SystemTransformatonPkg**".
3. Run the "**CPMerge.exe**".
4. Provide the Collection Point details.

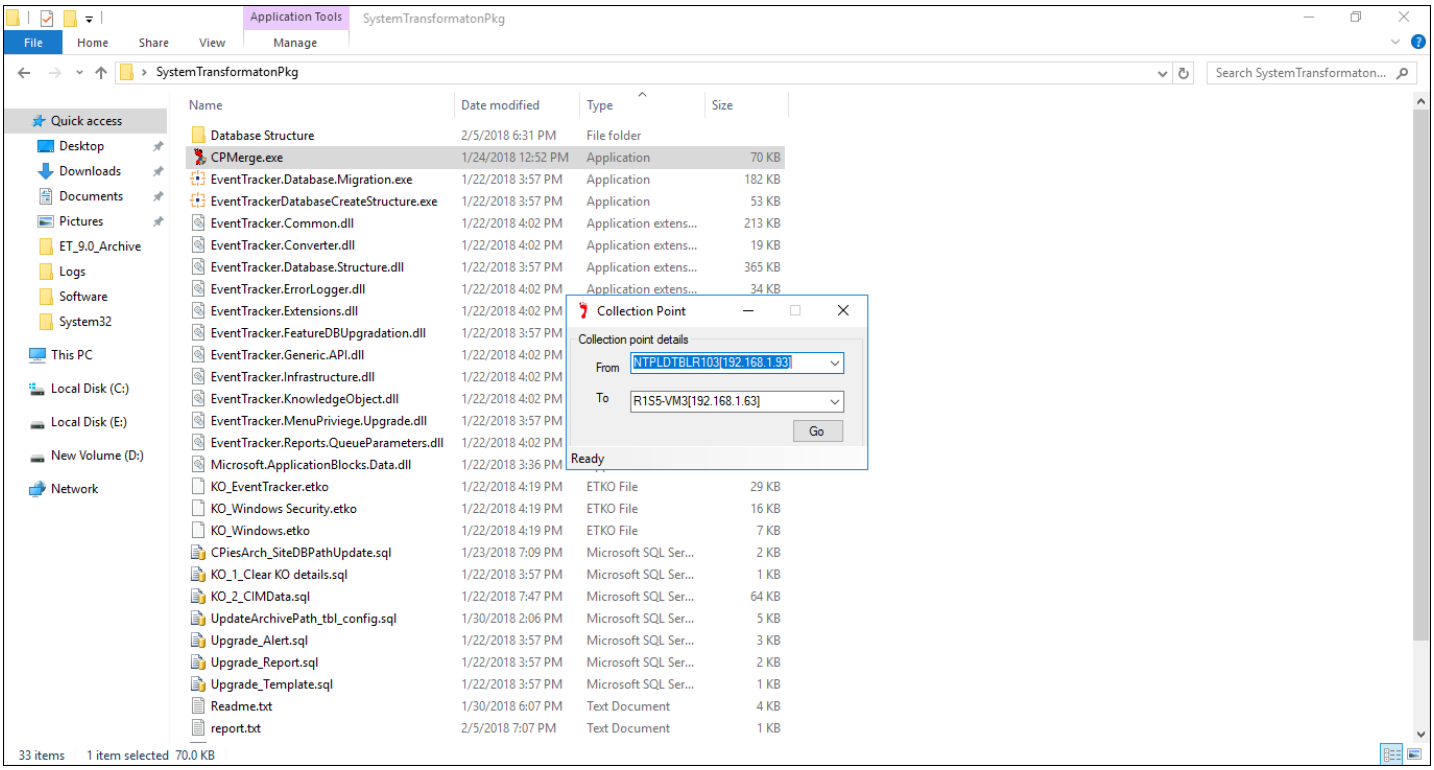


Figure 21

5. To start the merging, click on **GO**.

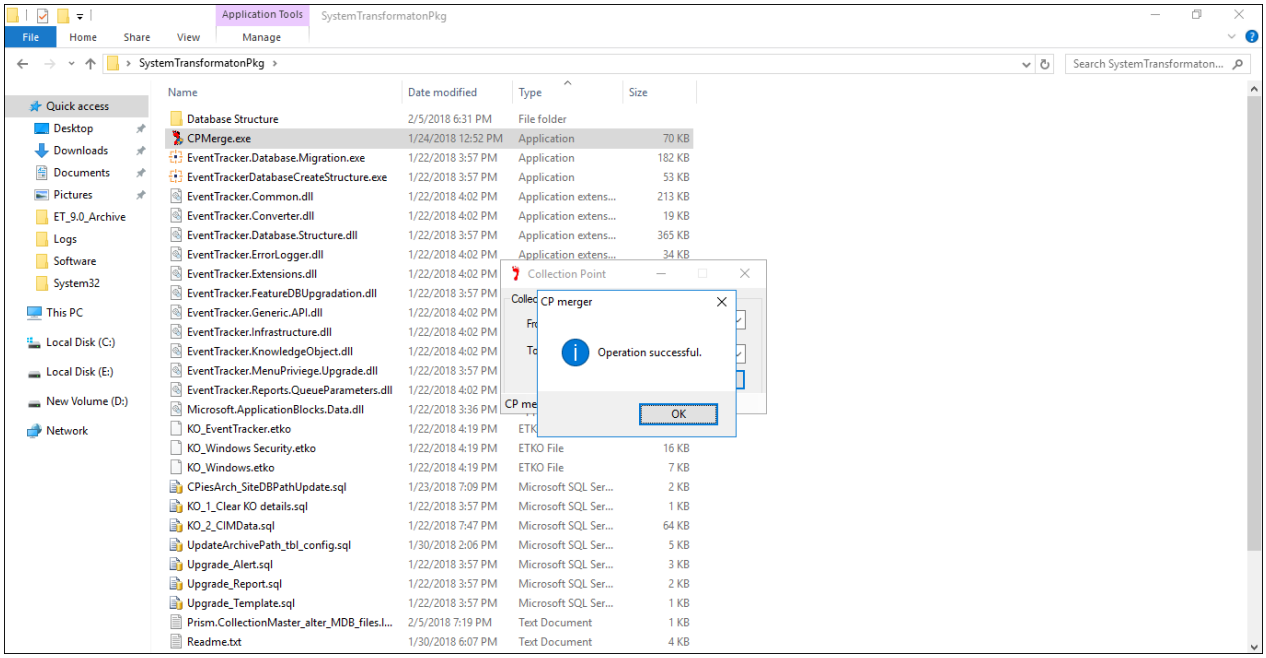


Figure 22

6. Once the CP merging is completed, it will show a success message as shown above.

Verify the merging in the **EventTracker Database**:

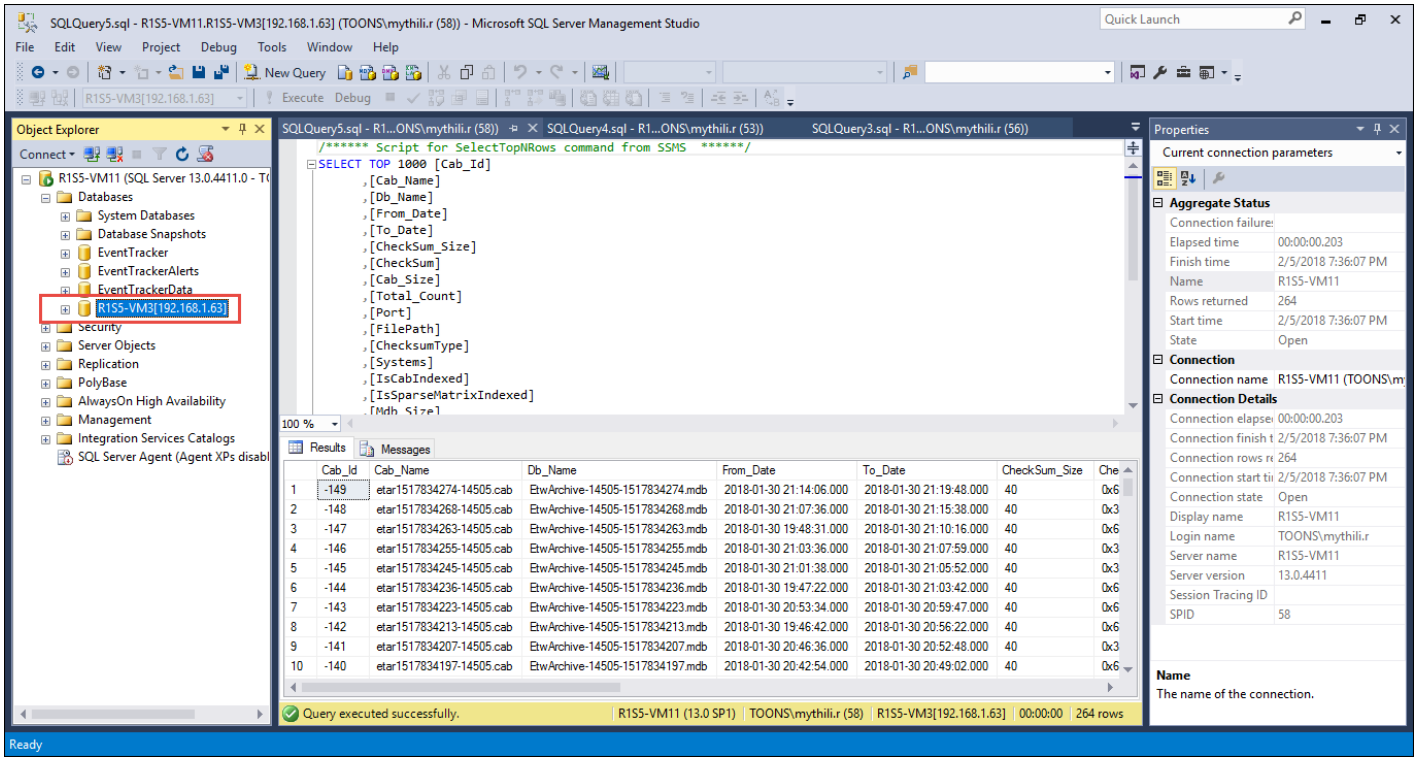


Figure 23

Verify the merged CP in the **EventTracker UI> Admin > Collection Master**:

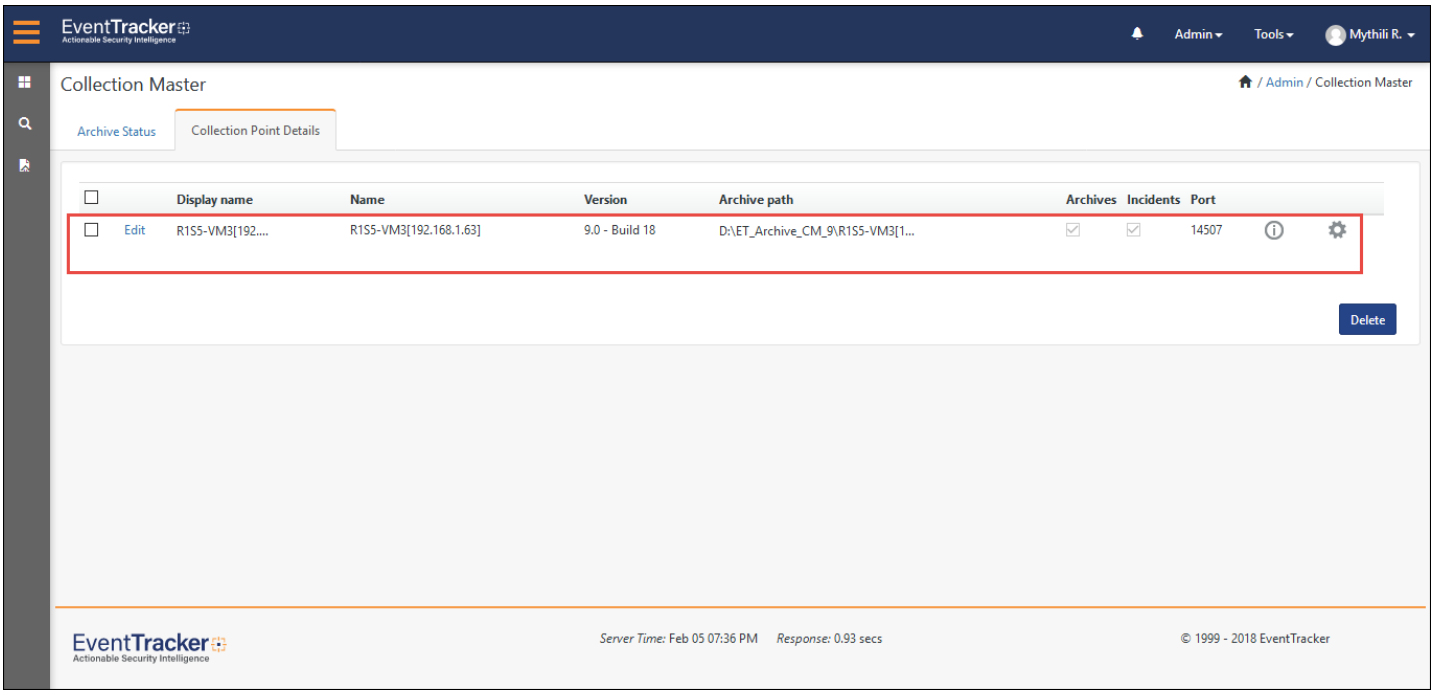


Figure 24

NOTE: After the Collection Point (CP) merging, if the old Site is not deleted in Database, then you have to delete it manually.

FAQ's

1. **Will there be a data loss during migration of EventTracker?**

   Yes. As we are stopping the EventTracker services in v8.2/v8.3 and 9.0 environments, there will be a downtime and data loss.

2. **What will happen to the LFM and DLA?**

   The user needs to re-configure the LFM and DLA after migration.

3. **Do we need to take a backup of the configuration files?**

   It is not mandatory. It is recommended to have a backup of your configuration files.