How to - Install EventTracker and Change Audit Agent

Agent Deployment User Manual
Abstract

EventTracker Agent deployment processes are described in detail in this manual for v 8.x and v7.x. EventTracker Agent can be deployed using methods like Active Directory Group Policy, Command Line, User Interface, and Manual Agent Install [Batch File Install]. The purpose of this document is to provide the step by step instructions to deploy EventTracker Agent using various methods and understand the deployment procedure.

Target audience

EventTracker users or system administrators, who wish to deploy the EventTracker Agent and Change Audit Agent.

Benefits/Advantages of EventTracker Windows Agent

- Monitoring application log files, TCP/UDP network activities, USB devices, VMware infrastructure, file and registry changes on the system
- Software install/uninstall
- Service start/stop
- Send events with guaranteed delivery (TCP)
- Performs automatic backup and clearing of the Windows Event Log
- Send events as syslog messages to UDP, TCP and TLS/SSL destinations
- Upload events as syslog formatted files to FTP, SFTP and SCP destinations
- Perform SCAP based configuration assessments
- Monitor file and registry changes on the system
# Table of Contents

Before You Begin ................................................................................................................. 6
Download and Prepare EventTracker Agent MSI Installer Package for Deployment .............................................. 8
EventTracker 8.2 ..................................................................................................................... 9
  Procedure to install with Agent.ini file .................................................................................. 14
  Procedure to install with Agent.ini and etaconfig.ini files .......................................................... 17
Deploy through Group Policy .................................................................................................. 22
  Before you Begin ................................................................................................................ 22
  Launch Group Policy Management Console ........................................................................... 26
  Create the Group Policy Object in Active Directory for Software Deployment .................... 26
Verify Installation .................................................................................................................. 37
  On Win XP, Win 2003 server operating systems .................................................................. 37
Limitation for Group Policy Installation .................................................................................... 39
How to deploy agent via Agent MSI in Server Core Machine? .................................................... 40
Deploy through Command Line ............................................................................................... 41
Deploy through User Interface ............................................................................................... 43
Uninstall EventTracker Agent ................................................................................................ 44
  How to launch EventTracker agent? ....................................................................................... 48
  How to launch Change Audit agent ...................................................................................... 49
Manual Agent install V8.2 [Batch File Install] ........................................................................ 49
Installing EventTracker Agent ............................................................................................... 49
  Preparing the files for manual agent installation .................................................................. 50
  Performing the installation on XP/2K3 .................................................................................. 50
  Performing the installation on Vista/2k8/Win7 when UAC is enabled ........................................... 50
  Performing the installation on Vista/2k8/Win7 (64 bit OS) ...................................................... 51
  Performing the installation on Win8/8.1/2012/10 (64 bit OS) ................................................. 51
  Preparing the files for manual agent installation (EventTracker Change Audit Agent) .............. 52
  Performing the installation on XP/2K3 .................................................................................. 52
  Performing the installation on Vista/2k8/Win7 when UAC is enabled ........................................... 52
  Performing the installation on 64 bit OS ............................................................................... 52
EventTracker 8.1 .................................................................................................................... 53
  Procedure to install with Agent.ini file .................................................................................. 59
  Procedure to install with Agent.ini and etaconfig.ini files .......................................................... 60
Deploy through Group Policy .................................................................................................. 64
Before you Begin

Launch Group Policy Management Console

Create the Group Policy Object in Active Directory for Software Deployment

Verify Installation

On Win XP, Win 2003 server operating systems


Limitation for Group Policy Installation

How to deploy agent via Agent MSI in Server Core Machine?

Deploy through Command Line

Deploy through User Interface

Uninstall EventTracker Agent

How to launch EventTracker agent?

How to launch Change Audit agent?

Manual Agent install V8.1 [Batch File Install]

Installing EventTracker Agent

Preparing the files for manual agent installation

Performing the installation on XP/2K3

Performing the installation on Vista/2k8/Win7 when UAC is enabled

Performing the installation on Vista/2k8/Win7 (64 bit OS)

Performing the installation on Win8/8.1/2012/10 (64 bit OS)

Preparing the files for manual agent installation (EventTracker Change Audit Agent)

Performing the installation on XP/2K3

Performing the installation on Vista/2k8/Win7 when UAC is enabled

Performing the installation on 64 bit OS

EventTracker 8.0

Procedure to install with Agent.ini file

Procedure to install with Agent.ini and etaconfig.ini files

 Deploy through Group Policy

Before you Begin

Launch Group Policy Management Console

Create the Group Policy Object in Active Directory for Software Deployment

Verify Installation

On Win XP, Win 2003 server operating systems


Limitation for Group Policy Installation

How to deploy agent via Agent MSI in Server Core Machine?

Deploy through Command Line

Verify Installation
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to deploy agent via Agent MSI in Server Core Machine?</td>
<td>173</td>
</tr>
<tr>
<td>Deploy through Group Policy</td>
<td>156</td>
</tr>
<tr>
<td>Uninstall EventTracker Agent</td>
<td>131</td>
</tr>
<tr>
<td>How to launch EventTracker agent?</td>
<td>137</td>
</tr>
<tr>
<td>How to launch Change Audit agent</td>
<td>138</td>
</tr>
<tr>
<td>Manual Agent install V8.0 [Batch File Install]</td>
<td>139</td>
</tr>
<tr>
<td>Installing EventTracker Agent</td>
<td>139</td>
</tr>
<tr>
<td>Preparing the files for manual agent installation</td>
<td>139</td>
</tr>
<tr>
<td>Performing the installation on XP/2K3</td>
<td>140</td>
</tr>
<tr>
<td>Performing the installation on Vista/2k8/W7 when UAC is enabled</td>
<td>140</td>
</tr>
<tr>
<td>Performing the installation on Vista/2k8/W7 (64 bit OS)</td>
<td>140</td>
</tr>
<tr>
<td>Performing the installation on WinB/8.1/2012/10 (64 bit OS)</td>
<td>141</td>
</tr>
<tr>
<td>Preparing the files for manual agent installation (EventTracker Change Audit Agent)</td>
<td>141</td>
</tr>
<tr>
<td>Performing the installation on XP/2K3</td>
<td>141</td>
</tr>
<tr>
<td>Performing the installation on Vista/2k8/W7 when UAC is enabled</td>
<td>141</td>
</tr>
<tr>
<td>Performing the installation on 64 bit OS</td>
<td>142</td>
</tr>
<tr>
<td>EventTracker 7.6X</td>
<td>142</td>
</tr>
<tr>
<td>Procedure to install with Agent.ini file</td>
<td>150</td>
</tr>
<tr>
<td>Procedure to install with Agent.ini and etaconfig.ini files</td>
<td>151</td>
</tr>
<tr>
<td>Deploy through User Interface</td>
<td>130</td>
</tr>
<tr>
<td>Before you Begin</td>
<td>156</td>
</tr>
<tr>
<td>Launch Group Policy Management Console</td>
<td>156</td>
</tr>
<tr>
<td>Create the Group Policy Object in Active Directory for Software Deployment</td>
<td>159</td>
</tr>
<tr>
<td>Verify Installation</td>
<td>160</td>
</tr>
<tr>
<td>On Win XP, Win 2003 server operating systems</td>
<td>170</td>
</tr>
<tr>
<td>Limitation for Group Policy Installation</td>
<td>171</td>
</tr>
<tr>
<td>How to deploy agent via Agent MSI in Server Core Machine?</td>
<td>173</td>
</tr>
<tr>
<td>Deploy through Command Line</td>
<td>174</td>
</tr>
<tr>
<td>Deploy through User Interface</td>
<td>176</td>
</tr>
<tr>
<td>Uninstall EventTracker Agent</td>
<td>178</td>
</tr>
<tr>
<td>How to launch EventTracker agent?</td>
<td>183</td>
</tr>
<tr>
<td>How to launch Change Audit agent</td>
<td>184</td>
</tr>
<tr>
<td>Manual Agent install V7.6 [Batch File Install]</td>
<td>185</td>
</tr>
<tr>
<td>Installing EventTracker Agent</td>
<td>185</td>
</tr>
<tr>
<td>Preparing the files for manual agent installation</td>
<td>185</td>
</tr>
<tr>
<td>Performing the installation on XP/2K3</td>
<td>186</td>
</tr>
<tr>
<td>Performing the installation on Vista/2k8/W7 when UAC is enabled</td>
<td>186</td>
</tr>
</tbody>
</table>
EventTracker Agent Deployment

- Performing the installation on Vista/2k8/Win7 (64 bit OS) ................................................................. 186
- Performing the installation on Win8 (32 bit OS) .................................................................................. 186
- Performing the installation on Win8/8.1/2012 (64 bit OS) ............................................................... 187
- EventTracker Change Audit Agent installation (Manual): ................................................................. 187
  - Preparing the files for manual agent installation ............................................................................ 187
  - Performing the installation on XP/2K3 ......................................................................................... 187
  - Performing the installation on Vista/2k8/Win7 when UAC is enabled ...................................... 187
  - Performing the installation on 64 bit OS .................................................................................. 188
- EventTracker 7.5X ............................................................................................................................... 189
- Deploy through Command Line .......................................................................................................... 190
- Deploy through User Interface ............................................................................................................ 191
  - Procedure to install with Agent.ini file ..................................................................................... 196
  - Procedure to install with Agent.ini and etaconfig.ini files ......................................................... 197
- Deploy through Group Policy ............................................................................................................. 202
  - Before you Begin ......................................................................................................................... 202
  - Launch Group Policy Management Console ............................................................................. 205
  - Create the Group Policy Object in Active Directory for Software Deployment ..................... 206
  - Verify Installation ......................................................................................................................... 216
  - On Win XP, Win 2003 server operating systems ........................................................................ 216
- Limitation for Group Policy Installation ............................................................................................ 218
- Manual Agent Install V7.5 [Batch File Install] .................................................................................. 219
  - Installing EventTracker Agent ..................................................................................................... 219
  - Manual Agent Installation Using ‘psexec.exe’ .............................................................................. 221
    - Execute the batch file ................................................................................................................ 221
    - Install agents from 32 Bit Systems .......................................................................................... 221
    - Install agents from 64 Bit Systems ......................................................................................... 221
  - Installing Change Audit Agent .................................................................................................... 222
  - Change Audit Agent Installation Using ‘psexec.exe’ .................................................................. 224
    - Execute the batch file ................................................................................................................ 224
    - Install agents from 32 Bit Systems .......................................................................................... 224
    - Install agents from 64 Bit Systems ......................................................................................... 224
  - Uninstall EventTracker Agent ........................................................................................................ 225
  - Uninstall via Add or Remove Programs ....................................................................................... 225
  - Uninstall via Group Policy ........................................................................................................... 227
Before You Begin

Before you begin with EventTracker agent deployment, there are few things you need to have and do. Please keep in mind the points described below,

- Ensure that the EventTracker Scheduler service of EventTracker Manager is running during the installation process.

- Network Share, where the EventTracker agent MSI files are stored should be accessible from all the target systems.

- Domain systems should have at least read access on Network Share, where the EventTracker MSI files are stored.

- Target system(s) should be member of the same domain.

- Once EventTracker agents are installed via group policy, you will not be able to uninstall the agents from the EventTracker system manager.

- If agent is deployed via command line and UI, then it has to be uninstalled from Control Panel or from All Programs from Start.

- To use all features of EventTracker Agent, .NET Framework should be installed as per system requirement.

- It is recommended to install EventTracker and Change Audit either by command line, System Manager or by group policy.

- An option has been provided in v 8.0 where License will be fetched from License server provided in the configuration file. Hence, it is not required to copy the certificate file where the MSI package is present.

- For Windows 8/8.1 and Windows 2012, all the necessary windows update should be applied otherwise .Net 3.5 will not get installed using the MSI package.

- For Windows 8/8.1/2012/2012 R2/10, if .Net 3.5(which includes .Net 2.0 and .Net 3.0) is not present, then the user will need to install it manually. (Both for MSI and GPO)

- The new snapshots required for Change Audit will be taken at 2AM.

- To complete the installation, target system(s) need to be restarted after configuring software deployment policy.

- In Windows XP, sometimes it will take two reboots to get application installed. This is because Windows XP operates (by default) in a mode called Fast Logon Optimization. This
means that the computer boots and logs in quicker, but it does mean that events that should occur during the computer's boot or login will be delayed until the second boot or login.

- If the user wants to use config assessment then make sure that MSXML parser is available in that particular system.
  Approaches for installing MSXML parser-
  - Ensure that the windows updates are up to date.
  - Manually install MSXML parser.

- After installing .NET 3.5, the system will restart automatically. In case after .NET 3.5 is installed and the system prompts to restart, it is mandatory to restart the system and then continue with EventTracker installation.

- The latest MSI package **v 8.2 Build 14**, if the user uninstalls through System Manager, both the features (EventTracker Agent and Change Audit) will get uninstalled. In case the user selects any one of the features and tries to uninstall, it will uninstall the complete MSI package (where all components of the MSI package are similar to the manager agent components).

- For **v8.2, Build 14**, if the user is enabling minimal GUI option in agent.ini, all the essential parameters must be filled in the ini.
  - If the essential parameters are not filled by the users properly, it will display the warning message **'Please provide essential parameters in Agent.ini to proceed with the installation.'**
  - If the agent.ini is filled partially by the user, it will install the user selected feature (EventTracker Agent) completely and the not selected feature (ChangeAudit) will be installed partially.

- For v8.1 Build 9 and v8.0 Build 29, while configuring VMware, it throws an error message, which is displayed below:

  ![Error connecting to the VMware server](image)

  Then, the user will have to register **EtVMagent.dll**.
To register, please follow the below steps:

- Change the directory to the location where Agent is deployed.
- Type the Command
  
  ```
  Regasm EtVMagent.dll
  ```
- After registering a message will be displayed as shown below:
  
  “Types registered successfully”

**NOTE:**

Before deploying the EventTracker Agent, it is recommended that the EventTracker Scheduler service of EventTracker Manager is running during the installation process. This should be done so that the installer can connect with the EventTracker Manager and retrieve the license detail which is taken care of by the EventTracker Scheduler service. If, this is not done during the installation, you will not be able to access the EventTracker features that you opted for.

**Download and Prepare EventTracker Agent MSI Installer Package for Deployment**

Before you start with deployment, you need to extract MSI files to a suitable folder. Follow the instructions given below,
EventTracker 8.2

1. Download MSI package (e.g. AgentMSI_82.zip for v8.2) from the location provided by Prism Microsystems Support team.

   The details about other versions are mentioned in table below. Refer Table 1.

2. Extract AgentMSI_82.zip to AgentMSI_82/.

3. Fill the necessary details in ‘Agent.ini’ configuration file (refer Table 2 on how to specify the parameters).

<table>
<thead>
<tr>
<th>EventTracker Agent Version</th>
<th>Zip file name</th>
<th>Executable file</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2</td>
<td>AgentMSI_82.zip</td>
<td>etwAgent82.exe</td>
</tr>
<tr>
<td>8.1</td>
<td>AgentMSI_81.zip</td>
<td>etwAgent81.exe</td>
</tr>
<tr>
<td>8.0</td>
<td>AgentMSI_80.zip</td>
<td>etwAgent80.exe</td>
</tr>
</tbody>
</table>

Table 1

Deploy through Command Line

1. To launch command line, click the Start button, and then click Run.

2. In Run dialog box, type ‘CMD’, and then click the Ok button.

3. Change directory to AgentMSI_82.

4. Type ‘EventTrackerAgent.msi /qn’ command, and then click the Enter button.
NOTE:

- For Windows 8/8.1 and Windows 2012 operating system, .Net 3.5 will be enabled using a batch file provided in MSI package.

- All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently. If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file but the Suffix Name will be fetched from the Agent.ini file (in case the user has provided the suffix in agent.ini file).

- If agent.ini file does not contain any parameters, and etaconfig.ini file is also present in the same folder, then silent installation will not be successful.

- Agent.ini contains default value for shortcut as ‘0’; hence shortcut will not be created in startmenu. In order to get the shortcut in startmenu user has to manually change shortcut as ‘1’.

Deploy through User Interface

NOTE:

1. Click etwAgent.exe file for v8.2.
   InstallShield Wizard pop up window appears on the screen.

![InstallShield Wizard](Image)

Figure 2
The executable files for other versions are mentioned in Table 1.

2. Click the **Next >** button to start with installation.

![Figure 3](image-url)

3. Read the **License Agreement**, and then select the option **'I accept the terms in the license agreement'**.
4. Click the **Next >** button.

5. In **Custom Setup**, select **EventTracker Windows Agent** and **Change Audit Agent** based on the requirement.

   Refer Figure 5.
Click the icon to select the installation options:

- Select ‘**This feature will be installed on local hard drive**’ option to install only agent and not sub features.
- **OR**
- Select ‘**This feature, and all subfeatures, will be installed on local hard drive**’ option to install agent as well as its sub features.
- **OR**
- Select the ‘**This feature will not be available**’ option, if you do not wish to install the agent.

6. Click the **Change** button to change the installation path of the agent and then click the **Next >** button.
7. In the Event destination pane, there are two methods to install EventTracker and Change Audit agents:

- Procedure to install with Agent.ini file
- Procedure to install with Agent.ini and etaconfig.ini files

**Procedure to install with Agent.ini file**

a) Enter EventTracker Manager: (Ex. Win2k3x64), Port number: (Ex. 14505 to 14580).

b) Select Deploy SCAP / Deploy WINSCP option as per the requirement.

c) Enter License Server: (Ex. Win2k3x64), Port number: (Ex. 14503) and Change Audit Manager: (Ex. Win2k3x64).

d) Click the Next > button.

Refer Figure 10.
NOTE:

- If the agent.ini file has the proper inputs like manager name/port/license server etc.,
  the application reads the information from the file automatically and displays the same
  in UI. There is no need to enter the values, provided if any change is required.
- The Event Destination(Figure: 10) window will be hidden, if the user has filled the
  configuration details in agent.ini
- The user can change the License Server name as per convenience.

If only EventTracker Windows Agent is selected, the below screen gets displayed.
If only **Change Audit** is selected, the following window gets displayed.
Procedure to install with Agent.ini and etaconfig.ini files

a) To achieve this, first copy 'etaconfig.ini' file from "<INSTALLDIR>\EventTracker\Agent" folder to the same directory/folder where setup resides.

b) In Event destination pane, select Deploy SCAP / Deploy WINSCP option as per the requirement.

c) Enter Change Audit Manager: (Ex. Win2k3x64) details and then click the Next > button.
NOTE:

- If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file but the Suffix Name will be fetched from the Agent.ini file (In case the user has provided suffix in agent.ini file).

- Also, if the user doesn’t select SCAP or WINSCP, the agent will be installed with both the features.

8. In this last step of the installation process, click the **Install** button.
NOTE: If suffix is enabled in the Agent.ini file, the below figure will get displayed.

- If the user enters a suffix name in the Agent.ini file, then the name will be displayed in the "Please Enter Location name" field, by default. Also if the user wants to edit the suffix name, he/she can edit it in the below screen.
- If the user does not add any suffix name in the .ini file, the field will be displayed blank.
NOTE: Allowed special character: ‘-‘, ‘_’, ‘.’ and the characters are limited to 100.

9. In **Basic Configuration** dialog box, check the configuration options to apply to the manager system, and then click the **OK** button.

**NOTE:**

The **Basic Configuration** dialog box does not display if installation is carried out via `etaconfig.ini` file.

![Basic Configuration Dialog Box](image)

*Figure 11: Basic Configuration*
NOTE:

If the deployed agent machine is not able to connect to the License Server, then the Basic Configuration window will come as blank, as displayed in the below figure:

![Basic Configuration Window](image.png)

Figure 14

10. Click the **Finish** button to complete the installation process.
Deploy through Group Policy

Before you Begin

1. Modify `Agent.ini` and change **EM** (ENTERPRISE_MANAGER), **CM** (Change Audit manager), **INSTALLDIR** (EventTracker Agent install directory) **EP** (ENTERPRISE_PORT), **LS** (License server name/ IP Address where the digital certificate is installed), and **LP** (License server port number) value appropriately.

<table>
<thead>
<tr>
<th>Configuration Settings</th>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>[INSTALL_PATH]</td>
<td>[INSTALL_PATH]</td>
</tr>
<tr>
<td>INSTALLDIR=&lt;Installation directory if agent need to be</td>
<td>INSTALLDIR=</td>
</tr>
<tr>
<td>installed in other than default path&gt;</td>
<td></td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[ENTERPRISE_MANAGER]</td>
<td>[ENTERPRISE_MANAGER]</td>
</tr>
<tr>
<td>EM=&lt;EventTracker Manager Hostname or IP Address&gt;</td>
<td>EM=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[ENTERPRISE_PORT]</td>
<td>[ENTERPRISE_PORT]</td>
</tr>
<tr>
<td></td>
<td>EP=14580</td>
</tr>
<tr>
<td></td>
<td>[END]</td>
</tr>
</tbody>
</table>
2. Create a network share on server and allow **Domain Computers** to have at least **READ** access permission.

3. Copy the **AgentMSI_82** folder to the network share, which is created in previous step.
Network share folder should have the below files.

![Folder Contents](image)

**Acronyms Used:**

- **INSTALLDIR:** If this parameter is left blank, the files will be installed in the default location i.e. `%ProgramFiles%\Prism Microsystems`.
- Else you can specify the path where you wish to install the files.
- **EM:** If this parameter is left blank, Enterprise manager won’t be installed.
- **EP:** If this parameter is left blank, the installer will assume the default port.
- **CM:** If this parameter is left blank, Change Audit manager won’t be installed.
- **IR:** If 1 then remedial actions are installed, if 0 then remedial actions are not installed. If this parameter is left blank, the installer takes a default value as “1”.
- **LS:** The system name/IP Address where the digital certificate is installed. If this parameter is left blank, the value will be read from EM (i.e. License server name will be the same as Enterprise manager)
- **LP:** If this parameter is left blank, the default port (i.e. 14503) will be assumed by the installer.
- **DS:** Deploy SCAP components. If the value is empty, then SCAP components will not be installed. If the value is ‘0’ or ‘1’, then SCAP components will be installed.
- **DW:** Deploy WINSCP components. If the value is empty then WINSCP components will not be installed. If the value is ‘0’ or ‘1’, then WINSCP components will be installed.
- **SC**: Shortcut will not be created in startmenu, if the value is ‘0’ or empty. If the value is ‘1’, then shortcut will be created in startmenu.

- **MG**: Setup wizard with minimal GUI, if the value is ‘1’. If the value is ‘0’, it means full GUI wizard.

- **IS SUFFIX**: Will ask for Suffix enabled or not. If the value is ‘0” it will be disabled and if the value is ‘1” it will be enabled.

- **SUFFIX**: Enter the system suffix name in this field.

**NOTE:**

- All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently.

- It is mandatory to specify either **Enterprise Manager** name or **Change Audit Manager** name.

- If user wish to install **EventTracker Agent** then Enterprise Manager Name (EM) is mandatory.

- If user wish to install **Change Audit Agent** then Change Audit Manager Name (CM) is mandatory.

- **Remedial Actions** are scripts or EXEs that can be launched at either the Agent or Manager Side, in response to events. If this option is enabled, predefined scripts will be placed in the **EventTracker\Agent\Script folder**.

- All checkbox setting in GUI like ‘Deploy SCAP components”, ‘Deploy WINSCP components”, “Remedial Actions components” will populate as per Agent.ini configuration.

- **Microsoft XML Core Services (MSXML)** is installed along with the MSI Agent Installer setup for 32-bit and 64-bit machines respectively.

- The **Microsoft Visual C++ 2008 Redistributable Package (x86)** which installs runtime components of **Visual C++ Libraries** required to run applications developed with Visual C++ is also installed along with the MSI Agent Installer setup.

- Before deploying the Agent, make sure that the Agent system(s) and domain controller are synchronized.

- For silent/GPO installation- installation will aborted if suffix/location name enable in Agent.ini and it value is empty.
Launch Group Policy Management Console

1. Select the Start button, select Settings, and then select Control Panel.
2. Select Administrative Tools, and then select Group Policy Management.

![Group Policy Management Console](image)

Figure 17

Create the Group Policy Object in Active Directory for Software Deployment

Follow the steps given below to create the new ‘Group Policy Object’ using the ‘Group Policy Management’ Snap-in,

1. In the Group Policy Management pane, expand Domains node, and then expand domain system node.
2. Right click **Group Policy Objects**, and then click **New**.

![Figure 18: Create Group Policy Object](image)

3. Enter a name for this new GPO (Ex. AgentMSI GPO) and then click the **OK** button.

![Figure 19: New GPO](image)

4. Click the name of newly created GPO. In this case, ‘AgentMSI GPO’.
A. In the **Security Filtering** pane, click the **Add** button to apply GPO settings to the domain computers group (or ensure the authenticated users group is listed).

B. In the **Enter the object name to select** field, type the object name or a part of the object name, and then click the **Check Names** button to select the object name.
C. Click the OK button.

5. Right click the newly created GPO, and then click Edit.

**Group Policy Object Editor** window will be opened.

A. Expand the **Computer Configuration**, and open **Software Settings**.

![Figure 22: Computer Configuration](image)

B. Right-click **Software Installation**, select **New**, and then select **Package**.

![Figure 23: Software installation, create new package](image)

**Open** window displays.
A. Locate the UNC path of the server share where the MSI installer file is located (\Server\Share\AgentMSI_82).

B. Select the MSI installer file EventTrackerAgent.msi, and then click Open.

EventTracker displays ‘Deploy Software’ dialog box. Refer Figure 25.

6. Select Assigned, and then click OK.

You have now created and assigned the Package Object.
7. Right-click on the **Package Object**, and then select **Properties**.

8. Click the **Security** tab; select the **Add** button to add **Domain Computers** to provide security permissions.

   Refer Figure 26.

   ![Figure 26](image)

9. Select the **Advanced** button, select **Find Now**.

   Refer Figure 27.
10. Select Domain Computers from Search results, and then select OK button.

11. Select the OK button.

12. In EventTrackerAgent Properties pane, select Read and Write permissions. Select the Advanced button.
Refer Figure 29.

**NOTE:**
Ensure **Domain Computers** has the **Read** and **Write** rights.

13. Select **Domain Computers**, and then click **Edit**.

Refer Figure 30.
14. Check the **List Contents**, **Read All Properties**, and **Read Permissions** options, if not selected. Select the **OK** button.

Refer Figure 30.

15. Select the **Apply** button and then select the **OK** button.

16. In **Group Policy Management** pane, right click the domain system name, and then select **New Organizational Unit** (OU).

A New Organizational Unit has to be created. Refer Figure 31.
17. Enter **New Organizational Unit** name.
   For example: Group Policy.

18. Right click newly created OU, and then click **Link an Existing GPO**.
    Refer Figure 32.
**NOTE:** Enable Enforced as ‘Yes’.

- Navigate to Linked GPO, right-click and enable the Enforced.

19. In the Select GPO dialog box, select the appropriate domain name and newly created Group Policy Object, and then click the OK button.


   The MSI package has now been defined and is ready for the deployment.

21. Force replication to all other domain controllers.

**NOTE:**

EventTracker and Change Audit Agents will be installed once the target machines are restarted.

If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
Verify Installation

Events will be sent to the target systems (i.e. "Manager" systems) upon successful deployment of EventTracker/ Change Audit agents. The name of the deployed agent along with their version number will appear in the System manager screen. On Target systems, following events will be generated in System Event Log:

On Win XP, Win 2003 server operating systems

On successful Agent deployment:

Example 1:

Event Type : Information
Event Source : Application Management
Event Category: None
Event ID : 301
User : NT AUTHORITY\SYSTEM
Computer : ESXWINXPVM8
Description : The assignment of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

Example 2:

Event Type : Information
Event Source : Application Management
Event Category: None
Event ID : 302
User : NT AUTHORITY\SYSTEM
Computer : ESXWINXPVM8
Description : The install of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

On Failed Agent deployment:

Event Type : Warning
EventTracker Agent Deployment

Event Source: Application Management
Event Category: None
Event ID: 102
User: NT AUTHORITY\SYSTEM
Computer: ESXWINXPVM8
Description: The install of application EventTrackerAgent from policy Software Deployment policy failed.


On Successful Agent Deployment:

Example 1:
Log Name: System
Source: Application Management Group Policy
Event ID: 301
Task Category: None
Level: Information
Keywords: Classic
User: SYSTEM
Computer: Esxwin2k8r2vm3.Toons.local
Description: The assignment of application EventTrackerAgent from policy Software Deployment policy succeeded.

Example 2:
Log Name: System
Source: Application Management Group Policy
Event ID: 302
Task Category: None
Level: Information
Keywords: Classic
User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy succeeded.

On Failed Agent Deployment:
Log Name : System
Source : Application Management Group Policy
Event ID : 102
Task Category : None
Level : Error
Keywords : Classic
User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.

Limitation for Group Policy Installation

- Retain configuration does not work via Group policy
- Upgrade agents is not supported via Group policy
- Modification features are not supported via Group policy
- Command line or silent installation doesn't support retain, upgrade and modify functions
- If EventTracker and Change Audit agent is installed via group policy then it is not possible to configure group policy to uninstall Change Audit or EventTracker agent only. While uninstalling both EventTracker and Change Audit agent will be uninstalled.
- GPO: shortcut value in agent.ini has to be kept as ‘One”, in case the user wants to uninstall agent from individual systems.
- GPO: In case the user wants to uninstall agent from all the systems using GPO uninstall option, then the shortcut value in agent.ini need not be changed.
How to deploy agent via Agent MSI in Server Core Machine?

1. Login to the server core system.

2. Copy the MSI package in the drive of server core machine. Make sure that the user has permission to the system.

3. Extract `AgentMSI_82.zip` to `AgentMSI_82\`.

4. Open Task Manager by pressing the key combinations **Ctrl + Shift + Esc**.

5. Click Run New Task from File Menu.

6. To open Command prompt, type **CMD** in the Create New Task Screen.
7. The Command Prompt Screen will be displayed.

**Deploy through Command Line**

1. To locate the MSI package, type the following commands:
   
   a. Exit from the **System 32** folder by typing the command `Cd\`
   
   b. Change the directory to **Agentmsi_82** by entering the command `Cd Agentmsi_82`.
   
   c. Now, open the **Agent.ini** file by typing `Agent.ini`.

![Create new task dialog box](image)

![Command Prompt Screen](image)
The Agent.ini file will be displayed.

2. Fill the necessary details in ‘Agent.ini’ configuration file.

![Agent.ini - Notepad](image)

**Figure 36**

3. Type ‘EventTrackerAgent.msi /qn’ command, and then click the Enter button.

![Administrator: C:\Windows\system32\cmd.exe](image)

**Figure 37**
Deploy through User Interface

1. Type `dir` to list the files that are available in the `Agentmsi_82` folder.

   The files inside the directory are listed.

2. Execute `etwAgent.exe` file by typing `etwAgent.exe`.

   ![Figure 39](image)

3. The EventTracker 8.2 InstallShield Wizard will get started.

   ![Figure 40](image)
4. To continue with the installation steps, please refer to Deploy through User Interface.

Uninstall EventTracker Agent

1. Open Task Manager by pressing the key combinations Ctrl + Shift + Esc.
2. Click Run New Task from File Menu.

![Task Manager Image]

Figure 41

3. Type regedit in the Create New Task Screen.

![Create New Task Image]

Figure 42
The **Registry Editor** screen will be displayed.

Go to the following location to find the registry keys:
*Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall*  

Figure 43

4. Traverse through all the registry keys until you find: 81
   - **DisplayName**: `EventTrackerAgent`
   - **InstallSource**: `AgentMSI_82`
5. Copy the key.

6. Open the Command Prompt and type `MsiExec.exe/uninstall` followed by the key.
7. Select **Yes** to confirm.

![Figure 46](image)

8. You will be asked whether to retain agent configuration settings. Click **Yes** if you wish to retain agent Configuration settings or else click **No**.

![Figure 47](image)

**NOTE:** In case you get the below message during the uninstall process, then the EventTracker and Change audit process has to be killed from task manager.
How to launch EventTracker agent?

1. Type `dir` to list the files that are available in the Agent folder.
   
   The files inside the directory are listed.

2. Type `etaconfig.exe` and press Enter to open EventTracker Agent Configuration.
How to launch Change Audit agent

1. Change directory to the path where \WcWindows\ folder is located.
2. Type `dir` to list the files that are available in the \WcWindows\ folder.
3. Type `WcWindows.exe` and press Enter to open EventTracker Change Audit Agent.

![Figure 51](image)

The EventTracker change audit agent is launched.

Manual Agent install V8.2 [Batch File Install]

Installing EventTracker Agent

**NOTE**

The agent installation procedure is applicable only for EventTracker V 8.2 users.
Preparing the files for manual agent installation

1. Extract the zip file in the root directory of install drive.

2. Replace Agent\AI\Temp\etaconfig.ini with your copy of etaconfig.ini.
   OR
   Specify the manager details in Agent\AI\Temp\etaconfig.ini

3. Specify the license server details in Agent\etsetup.ins. Open the file Agent\etsetup.ins in notepad and replace "LicServ_Name=\" with "LicServ_Name=<LicenseServerName>". Substitute the text "<LicenseServerName>" with the name/IP of manager system.

4. If program files shortcut menu is not required, then open the file Agent\etsetup.ins in notepad and replace "PgmMenuShortCutReq=1" with "PgmMenuShortCutReq=0".

5. If you do not want to install SCAP components on target system, then open the file Agent\etsetup.ins in notepad and replace "ETADeploySCAP=1" with "ETADeploySCAP=0".

6. If you do not want to install WinSCP components on target system, then open the file Agent\etsetup.ins in notepad and replace "ETADeployWinSCP=1" with "ETADeployWinSCP=0".

   The default etaconfig.ini available with this installer will not have a manager, license server configured, and File transfer, and Configuration assessment are disabled. If the default copy is not replaced, then please configure Manager and required settings by opening Programs-> EventTracker-> Agent Config (Agent Configuration GUI) or by running "etaconfig.exe" from installation path.

Performing the installation on XP/2K3

1. Execute install.bat.

Performing the installation on Vista/2k8/Win7 when UAC is enabled

1. Go to Start -> All Programs -> Accessories.

2. Right click on "Command Prompt" and select "Run as administrator" to open the command prompt as administrator.
3. In the command prompt change the directory to the path where `install.bat` file is located.

4. Type "install.bat" and press enter.

Performing the installation on Vista/2k8/Win7 (64 bit OS)

1. Open the file `Agent\etsetup.ins` and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

2. Execute `installx64.bat` (If UAC is enabled, see Performing the installation on Win8 (32 bit OS).

3. Performing the installation on Win8 (32 bit OS)

4. If you're using a keyboard with Windows 8, you can open an elevated Command Prompt from the Power User Menu. Just press the "WINDOWS" and "X" keys together and then click on "Command Prompt (Admin)".

5. Click "Yes" to the User Account Control message that appears.

6. In the command prompt, change the directory to the path where `install.bat` file is located.

7. Type "install.bat" and press enter.

**IMPORTANT NOTE:** Prior to installing agent on Win8 (32bit), user has to apply all important Windows updates which are related to .NET Framework 3.5.

Performing the installation on Win8/8.1/2012/10 (64 bit OS)

1. Open the file `Agent\etsetup.ins` and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

2. Execute `installx64.bat` (If UAC is enabled, see Performing the installation on Win8 (32 bit OS).

**IMPORTANT NOTE:** Prior to installing agent on Win8/8.1/2012 (64 bit), user has to apply all important Windows updates which are related to .NET Framework 3.5.
Preparing the files for manual agent installation (EventTracker Change Audit Agent)

1. Extract the zip file in the root directory of install drive.

2. Replace `Agent\AlTemp\wcw.ini` with your copy of `wcw.ini`.

3. Open the file `Agent\wcsetup.ins` in notepad and replace `Server=0"` with `"Server=<ManagerName>"`. Substitute the text `"<ManagerName>"` with the name of manager system.

4. If program files shortcut menu is not required, then open the file `Agent\wcsetup.ins` in notepad and replace `"PgmMenuShortCutReq=1"` with `"PgmMenuShortCutReq=0"`.

5. Specify the license server details in `Agent\wcsetup.ins`. Open the file `Agent\wcsetup.ins` in notepad and replace `"LicServ_Name=0"` with `"LicServ_Name=<LicenseServerName>"`. Substitute the text `"<LicenseServerName>"` with the name/IP of manager system.

Performing the installation on XP/2K3

1. Execute `install.bat`.

Performing the installation on Vista/2k8/Win7 when UAC is enabled

1. Go to `Start -> All Programs -> Accessories`.

2. Right click ‘Command Prompt" and select ‘Run as administrator" to open the command prompt as administrator.

3. In the command prompt change the directory to the path where `install.bat` file is located.

4. Type ‘`install.bat"` and press Enter.

Performing the installation on 64 bit OS

1. Open the file `Agent\wcsetup.ins` and update "`LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows`".

2. Execute `installx64.bat` (If UAC is enabled, see [Performing the installation on Vista/2k8/Win7 when UAC is enabled]).
EventTracker 8.1

4. Download MSI package (e.g. AgentMSI_81.zip for v8.1) from the location provided by Prism Microsystems Support team.

   The details about other versions are mentioned in table below. Refer **Table 1**.

5. Extract **AgentMSI_81.zip** to **AgentMSI_81\**.

6. Fill the necessary details in ’**Agent.ini’** configuration file (refer **Table 2** on how to specify the parameters).

![Figure 13](image)

<table>
<thead>
<tr>
<th>EventTracker Agent Version</th>
<th>Zip file name</th>
<th>Executable file</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0</td>
<td>AgentMSI_80.zip</td>
<td>etwAgent80.exe</td>
</tr>
<tr>
<td>8.1</td>
<td>AgentMSI_81.zip</td>
<td>etwAgent81.exe</td>
</tr>
</tbody>
</table>

**Table 1**

Deploy through Command Line

5. To launch command line, click the **Start** button, and then click **Run**.

6. In **Run** dialog box, type ’**CMD**’, and then click the ’**Ok**’ button.

7. Change directory to **AgentMSI_81**.

8. Type ’**EventTrackerAgent.msi /qn**’ command, and then click the **Enter** button.
NOTE:

- For Windows 8/8.1 and Windows 2012 operating system, .Net 3.5 will be enabled using a batch file provided in MSI package.
- All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently. If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
- If agent.ini file does not contain any parameters, and etaconfig.ini file is also present in the same folder, then silent installation will not be successful.
- Agent.ini contains default value for shortcut as '0'; hence shortcut will not be created in startmenu. In order to get the shortcut in startmenu user has to manually change shortcut as '1'.

Deploy through User Interface

NOTE:

On Vista, Win 7, Win 8, Win 2008, Win 2008 R2, Win 2012 and Win 2012 R2 operating systems, the MSI Installer executable should run with 'Administrative' privileges.

11. Click **etwAgent.exe** file for v8.1.

**InstallShield Wizard** pop up window appears on the screen.
The executable files for other versions are mentioned in Table 1.

12. Click the **Next >** button to start with installation.

![EventTracker 8.1 setup screen](image)

**Figure 15**

13. Read the **License Agreement**, and then select the option ‘**I accept the terms in the license agreement**’.
14. Click the **Next >** button.

15. In **Custom Setup**, select **EventTracker Windows Agent** and **Change Audit Agent** based on the requirement.

Refer Figure 5.
Click icon to select the installation options:

- Select 'This feature will be installed on local hard drive' option to install only agent and not sub features.

  OR

- Select 'This feature, and all subfeatures, will be installed on local hard drive' option to install agent as well as its sub features.

  OR

- Select the 'This feature will not be available' option, if you do not wish to install the agent.
16. Click the **Change** button to change the installation path of the agent and then click the **Next >** button.

17. In the **Event destination** pane, there are two methods to install EventTracker and Change Audit agents:

   - **Procedure to install with Agent.ini file**
   - **Procedure to install with Agent.ini and etaconfig.ini files**
Procedure to install with Agent.ini file

e) Enter **EventTracker Manager:** (Ex. Win2k3x64), **Port number:** (Ex. 14505 to 14580).

f) Select **Deploy SCAP/Deploy WINSCP** option as per the requirement.

g) Enter **License Server:** (Ex. Win2k3x64), **Port number:** (Ex. 14503) and **Change Audit Manager:** (Ex. Win2k3x64).

h) Click the **Next >** button.

Refer Figure 10.

![Figure 20: Event Destination](image)

**NOTE:**

- If the agent.ini file has the proper inputs like manager name/port/license server etc., the application reads the information from the file automatically and displays the same in UI. There is no need to enter the values, provided if any change is required.
• The Event Destination(Figure: 10) window will be hidden, if the user has filled the configuration details in agent.ini

Procedure to install with Agent.ini and etaconfig.ini files

d) To achieve this, first copy ‘etaconfig.ini’ file from”<INSTALLDIR>\EventTracker\Agent“ folder to the same directory/folder where setup resides.

e) In Event destination pane, select Deploy SCAP / Deploy WINSCP option as per the requirement.

f) Enter Change Audit Manager: (Ex. Win2k3x64) details and then click the Next > button.

NOTE:
• If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
Also, if the user doesn't select SCAP or WINSCP, the agent will be installed with both the features.

18. In this last step of the installation process, check the 'Install default Remedial action EXEs on this machine' option, and then click the Install button.

**NOTE:**

To select 'Install default Remedial action EXEs on this machine' option is not mandatory. If you do not wish to enable remedial action then do not select the option. Directly click the Install button.

19. In Basic Configuration dialog box, check the configuration options to apply to the manager system, and then click the OK button.

**NOTE:**

The Basic Configuration dialog box does not display if installation is carried out via etaconfig.ini file.
NOTE:

If the deployed agent machine is not able to connect to the License Server, then the Basic Configuration window will come as blank, as displayed in the below figure:
20. Click the **Finish** button to complete the installation process.
Deploy through Group Policy

Before you Begin

4. Modify Agent.ini and change **EM** (ENTERPRISE_MANAGER), **CM** (Change Audit manager), **INSTALLDIR** (EventTracker Agent install directory) **EP** (ENTERPRISE_PORT), **LS** (License server name/IP Address where the digital certificate is installed), and **LP** (License server port number) value appropriately.

<table>
<thead>
<tr>
<th>Configuration Settings</th>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>[INSTALL_PATH]</td>
<td>[INSTALL_PATH]</td>
</tr>
<tr>
<td>INSTALLDIR=</td>
<td>INSTALLDIR=</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[ENTERPRISE_MANAGER]</td>
<td>[ENTERPRISE_MANAGER]</td>
</tr>
<tr>
<td>EM=</td>
<td>EM=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[ENTERPRISE_PORT]</td>
<td>[ENTERPRISE_PORT]</td>
</tr>
<tr>
<td>EP=</td>
<td>EP=14500</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[CHANGE_AUDIT_MANAGER]</td>
<td>[CHANGE_AUDIT_MANAGER]</td>
</tr>
<tr>
<td>CM=</td>
<td>CM=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[REMEDIAL_ACTIONS]</td>
<td>[REMEDIAL_ACTIONS]</td>
</tr>
<tr>
<td>IR=1</td>
<td>IR=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[LICENSE_SERVER]</td>
<td>[LICENSE_SERVER]</td>
</tr>
<tr>
<td>LS=</td>
<td>LS=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[LICENSE_SERVER_PORT]</td>
<td>[LICENSE_SERVER_PORT]</td>
</tr>
<tr>
<td>LP=</td>
<td>LP=14503</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>Deploy SCAP components</td>
<td>Deploy SCAP components</td>
</tr>
<tr>
<td>[DEPLOY_SCAP]</td>
<td>[DEPLOY_SCAP]</td>
</tr>
<tr>
<td>DS= '1' or '0'</td>
<td>DS=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>Deploy WINSCP components</td>
<td>Deploy WINSCP components</td>
</tr>
<tr>
<td>[DEPLOY_WINSCP]</td>
<td>[DEPLOY_WINSCP]</td>
</tr>
<tr>
<td>DW= '1' or '0'</td>
<td>DW=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>Create startmenu shortcut</td>
<td>Create startmenu shortcut</td>
</tr>
<tr>
<td>[SHORTCUT]</td>
<td>[SHORTCUT]</td>
</tr>
<tr>
<td>SC= '1' or '0'</td>
<td>SC=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
</tbody>
</table>

Table 2
5. Create a network share on server and allow **Domain Computers** to have at least **READ** access permission.

6. Copy the **AgentMSI_81** folder to the network share, which is created in previous step.

   Network share folder should have the below files.

![Folder Contents](image)

**Figure 24**

**Acronyms Used:**

- **INSTALLDIR**: If this parameter is left blank, the files will be installed in the default location i.e. `%ProgramFiles%\Prism Microsystems`.

- Else you can specify the path where you wish to install the files.

- **EM**: If this parameter is left blank, Enterprise manager won’t be installed.

- **EP**: If this parameter is left blank, the installer will assume the default port.

- **CM**: If this parameter is left blank, Change Audit manager won’t be installed.

- **IR**: If 1 then remedial actions are installed, if 0 then remedial actions are not installed. If this parameter is left blank, the installer takes a default value as “1”.

- **LS**: The system name/ IP Address where the digital certificate is installed. If this parameter is left blank, the value will be read from EM (i.e. License server name will be the same as Enterprise manager)

- **LP**: If this parameter is left blank, the default port (i.e. 14503) will be assumed by the installer.
• **DS**: Deploy SCAP components. If the value is empty, then SCAP components will not be installed. If the value is ‘0’ or ‘1’, then SCAP components will be installed.

• **DW**: Deploy WINSCP components. If the value is empty then WINSCP components will not be installed. If the value is ‘0’ or ‘1’, then WINSCP components will be installed.

• **SC**: shortcut will not be created in startmenu, if the value is ‘0’ or empty. If the value is ‘1’, then shortcut will be created in startmenu.

**NOTE:**

• All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently.

• It is mandatory to specify either **Enterprise Manager** name or **Change Audit Manager** name.

• If user wish to install **EventTracker Agent** then Enterprise Manager Name (**EM**) is mandatory.

• If user wish to install **Change Audit Agent** then Change Audit Manager Name (**CM**) is mandatory.

• **Remedial Actions** are scripts or EXEs that can be launched at either the Agent or Manager Side, in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder.

• All checkbox setting in GUI like ‘Deploy SCAP components”, ‘Deploy WINSCP components”, ‘Remedial Actions components” will populate as per Agent.ini configuration.

• **Microsoft XML Core Services (MSXML)** is installed along with the MSI Agent Installer setup for 32-bit and 64-bit machines respectively.

• The **Microsoft Visual C++ 2008 Redistributable Package (x86)** which installs runtime components of **Visual C++ Libraries** required to run applications developed with Visual C++ is also installed along with the MSI Agent Installer setup.

• Before deploying the Agent, make sure that the Agent system(s) and domain controller are synchronized.
Launch Group Policy Management Console

3. Select the **Start** button, select **Settings**, and then select **Control Panel**.
4. Select **Administrative Tools**, and then select **Group Policy Management**.

![Group Policy Management Console](image)
Create the Group Policy Object in Active Directory for Software Deployment

Follow the steps given below to create the new ‘Group Policy Object’ using the ‘Group Policy Management’ Snap-in,

22. In the Group Policy Management pane, expand Domains node, and then expand domain system node.

23. Right click Group Policy Objects, and then click New.

24. Enter a name for this new GPO (Ex. AgentMSI GPO) and then click the OK button.
25. Click the name of newly created GPO. In this case, ‘AgentMSI GPO’.

![Figure 20](image)

D. In the Security Filtering pane, click the Add button to apply GPO settings to the domain computers group (or ensure the authenticated users group is listed).

E. In the Enter the object name to select field, type the object name or a part of the object name, and then click the Check Names button to select the object name.
26. Right click the newly created GPO, and then click **Edit**.

   **Group Policy Object Editor** window will be opened.

   C. Expand the **Computer Configuration**, and open **Software Settings**.

   D. Right-click **Software Installation**, select **New**, and then select **Package**.

   F. Click the **OK** button.
Open window displays.

C. Locate the UNC path of the server share where the MSI installer file is located (\Server\Share\AgentMSI_81).  
D. Select the MSI installer file EventTrackerAgent.msi, and then click Open.

EventTracker displays ‘Deploy Software’ dialog box. Refer Figure 25.
27. Select **Assigned**, and then click **OK**.

You have now created and assigned the **Package Object**.

28. Right-click on the **Package Object**, and then select **Properties**.

29. Click the **Security** tab; select the **Add** button to add **Domain Computers** to provide security permissions.

Refer Figure 26.
30. Select the **Advanced** button, select **Find Now**.

Refer Figure 27.

![Figure 27](image1)

31. Select Domain Computers from Search results, and then select OK button.

![Figure 28](image2)

32. Select the **OK** button.
33. In **EventTrackerAgent Properties** pane, select **Read** and **Write** permissions. Select the **Advanced** button.
Refer Figure 29.

![EventTrackerAgent Properties](image)

**Figure 29**

**NOTE:**
Ensure **Domain Computers** has the **Read** and **Write** rights.

34. Select **Domain Computers**, and then click **Edit**.

Refer Figure 30.
35. Check the **List Contents**, **Read All Properties**, and **Read Permissions** options, if not selected. Select the **OK** button.

Refer Figure 30.

36. Select the **Apply** button and then select the **OK** button.

37. In **Group Policy Management** pane, right click the domain system name, and then select **New Organizational Unit** (OU).

A New Organizational Unit has to be created. Refer Figure 31.
38. Enter **New Organizational Unit** name.
   
   For example: Group Policy.

39. Right click newly created OU, and then click **Link an Existing GPO**.
   
   Refer Figure 32.
**NOTE:** Enable Enforced as ‘**Yes**’.

- Navigate to Linked GPO, right-click and enable the **Enforced**.

40. In the **Select GPO** dialog box, select the appropriate **domain name** and newly created **Group Policy Object**, and then click the **OK** button.

41. Close the **Group Policy window**.

   The **MSI package** has now been defined and is ready for the deployment.

42. Force replication to all other domain controllers.

**NOTE:**

EventTracker and Change Audit Agents will be installed once the target machines are restarted.

If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
Verify Installation

Events will be sent to the target systems (i.e. "Manager" systems) upon successful deployment of EventTracker/Change Audit agents. The name of the deployed agent along with their version number will appear in the System manager screen. On Target systems, following events will be generated in System Event Log:

On Win XP, Win 2003 server operating systems

On successful Agent deployment:

**Example 1:**

- **Event Type:** Information
- **Event Source:** Application Management
- **Event Category:** None
- **Event ID:** 301
- **User:** NT AUTHORITY\SYSTEM
- **Computer:** ESXWINXPVM8
- **Description:** The assignment of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

**Example 2:**

- **Event Type:** Information
- **Event Source:** Application Management
- **Event Category:** None
- **Event ID:** 302
- **User:** NT AUTHORITY\SYSTEM
- **Computer:** ESXWINXPVM8
- **Description:** The install of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

On Failed Agent deployment:

- **Event Type:** Warning
EventTracker Agent Deployment

Event Source : Application Management
Event Category: None
Event ID : 102
User : NT AUTHORITY\SYSTEM
Computer : ESXWINXPVM8
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.


On Successful Agent Deployment:

Example 1:
Log Name : System
Source : Application Management Group Policy
Event ID : 301
Task Category : None
Level : Information
Keywords : Classic
User : SYSTEM
Computer : Esxwin2k8r2vm3.Toons.local
Description : The assignment of application EventTrackerAgent from policy Software Deployment policy succeeded.

Example 2:
Log Name : System
Source : Application Management Group Policy
Event ID : 302
Task Category : None
Level : Information
Keywords : Classic
EventTracker Agent Deployment

User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy succeeded.

On Failed Agent Deployment:

Log Name : System
Source : Application Management Group Policy
Event ID : 102
Task Category : None
Level : Error
Keywords : Classic
User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.

Limitation for Group Policy Installation

- Retain configuration does not work via Group policy
- Upgrade agents is not supported via Group policy
- Modification features are not supported via Group policy
- Command line or silent installation doesn't support retain, upgrade and modify functions
- If EventTracker and Change Audit agent is installed via group policy then it is not possible to configure group policy to uninstall Change Audit or EventTracker agent only. While uninstalling both EventTracker and Change Audit agent will be uninstalled.
- GPO: shortcut value in agent.ini has to be kept as ‘One”, in case the user wants to uninstall agent from individual systems.
- GPO: In case the user wants to uninstall agent from all the systems using GPO uninstall option, then the shortcut value in agent.ini need not be changed.
How to deploy agent via Agent MSI in Server Core Machine?

8. Login to the server core system.

9. Copy the MSI package in the drive of server core machine. Make sure that the user has permission to the system.

10. Extract AgentMSI_81.zip to AgentMSI_81/.

11. Open Task Manager by pressing the key combinations Ctrl + Shift+ Esc.


13. To open Command prompt, type CMD in the Create New Task Screen.
14. The Command Prompt Screen will be displayed.

**Deploy through Command Line**

4. To locate the MSI package, type the following commands:
   
   d. Exit from the **System 32** folder by typing the command `Cd\`

   e. Change the directory to **Agentmsi_81** by entering the command `Cd Agentmsi_81`.

   f. Now, open the **Agent.ini** file by typing `Agent.ini`. 
The Agent.ini file will be displayed.

5. Fill the necessary details in ‘Agent.ini’ configuration file.
6. Type `EventTrackerAgent.msi /qn` command, and then click the Enter button.
Deploy through User Interface

5. Type `dir` to list the files that are available in the `Agentmsi_81` folder.

   The files inside the directory are listed.


   ![Figure 39](image)

7. The EventTracker 8.1 InstallShield Wizard will get started.
8. To continue with the installation steps, please refer to Deploy through User Interface.

Uninstall EventTracker Agent

9. Open Task Manager by pressing the key combinations Ctrl + Shift+ Esc.

11. Type `regedit` in the **Create New Task** Screen.

The **Registry Editor** screen will be displayed.
Go to the following location to find the registry keys:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\

12. Traverse through all the registry keys until you find: 81
   - DisplayName: **EventTrackerAgent**
   - Installsource: **AgentMSI_81**
13. Copy the key.

14. Open the Command Prompt and type `MsiExec.exe/uninstall` followed by the key.
15. Select **Yes** to confirm.

![Image of Windows Installer window](image)

**Figure 46**

![Image of EventTracker Agent configuration window](image)

**Figure 47**

16. You will be asked whether to retain agent configuration settings.  
   
   Click **Yes** if you wish to retain agent Configuration settings or else click **No**.
NOTE

In case you get the below message during the uninstall process, then the EventTracker and Change audit process has to be killed from task manager.

How to launch EventTracker agent?

3. Type `dir` to list the files that are available in the Agent folder.
   The files inside the directory are listed.

4. Type `etaconfig.exe` and press Enter to open EventTracker Agent Configuration.
How to launch Change Audit agent

4. Change directory to the path where *WcWindows* folder is located.

5. Type `dir` to list the files that are available in the *WcWindows* folder.

6. Type `WcWindows.exe` and press Enter to open EventTracker Change Audit Agent.
The EventTracker change audit agent is launched.

**Manual Agent install V8.1 [Batch File Install]**

**Installing EventTracker Agent**

**NOTE**

The agent installation procedure is applicable only for EventTracker V 8.1 users.

**Preparing the files for manual agent installation**

1. Extract the zip file in the root directory of install drive.

2. Replace `Agent\AI\Temp\etaconfig.ini` with your copy of `etaconfig.ini`.

OR
Specify the manager details in `Agent\AlTemp\etaconfig.ini`.

9. Specify the license server details in `Agent\etsetup.ins`. Open the file `Agent\etsetup.ins` in notepad and replace "LicServ_Name=" with "LicServ_Name=<LicenseServerName>". Substitute the text "<LicenseServerName>" with the name/IP of manager system.

10. If program files shortcut menu is not required, then open the file `Agent\etsetup.ins` in notepad and replace "PgmMenuShortCutReq=1" with "PgmMenuShortCutReq=0".

11. If you do not want to install SCAP components on target system, then open the file `Agent\etsetup.ins` in notepad and replace "ETADeploySCAP=1" with "ETADeploySCAP=0".

12. If you do not want to install WinSCP components on target system, then open the file `Agent\etsetup.ins` in notepad and replace "ETADeployWinSCP=1" with "ETADeployWinSCP=0".

The default `etaconfig.ini` available with this installer will not have a manager, license server configured, and File transfer, and Configuration assessment are disabled. If the default copy is not replaced, then please configure Manager and required settings by opening Programs-> EventTracker-> Agent Config (Agent Configuration GUI) or by running "etaconfig.exe" from installation path.

Performing the installation on XP/2K3

3. Execute `install.bat`.

Performing the installation on Vista/2K8/Win7 when UAC is enabled

5. Go to Start -> All Programs -> Accessories.

6. Right click on **Command Prompt** and select **Run as administrator** to open the command prompt as administrator.

7. In the command prompt change the directory to the path where `install.bat` file is located.

8. Type **install.bat** and press enter.
Performing the installation on Vista/2k8/Win7 (64 bit OS)

2. Open the file Agent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

4. Execute installx64.bat bat (If UAC is enabled, see Performing the installation on Win8 (32 bit OS).

4. Performing the installation on Win8 (32 bit OS)

8. If you’re using a keyboard with Windows 8, you can open an elevated Command Prompt from the Power User Menu. Just press the "WINDOWS" and "X" keys together and then click on "Command Prompt (Admin)".

9. Click “Yes” to the User Account Control message that appears.

10. In the command prompt, change the directory to the path where install.bat file is located.

11. Type “install.bat” and press enter.

IMPORTANT NOTE: Prior to installing agent on Win8 (32bit), user has to apply all important Windows updates which are related to .NET Framework 3.5.

Performing the installation on Win8/8.1/2012/10 (64 bit OS)

2. Open the file Agent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

3. Execute installx64.bat (If UAC is enabled, see Performing the installation on Win8 (32 bit OS).

IMPORTANT NOTE: Prior to installing agent on Win8/8.1/2012 (64 bit), user has to apply all important Windows updates which are related to .NET Framework 3.5.

Preparing the files for manual agent installation (EventTracker Change Audit Agent)

6. Extract the zip file in the root directory of install drive.

7. Replace Agent\AllTemp\wcw.ini with your copy of wcw.ini.
8. Open the file `Agent\wcsetup.ins` in notepad and replace “Server=0” with “Server=<ManagerName>”. Substitute the text “<ManagerName>” with the name of manager system.

9. If program files shortcut menu is not required, then open the file `Agent\wcsetup.ins` in notepad and replace “PgmMenuShortCutReq=1” with “PgmMenuShortCutReq=0”.

10. Specify the license server details in `Agent\wcsetup.ins`. Open the file `Agent\wcsetup.ins` in notepad and replace “LicServ_Name=0” with “LicServ_Name=<LicenseServerName>”. Substitute the text “<LicenseServerName>” with the name/IP of manager system.

Performing the installation on XP/2K3

2. Execute `install.bat`.

Performing the installation on Vista/2k8/Win7 when UAC is enabled

5. Go to Start -> All Programs -> Accessories.

6. Right click ‘Command Prompt” and select ‘Run as administrator” to open the command prompt as administrator.

7. In the command prompt change the directory to the path where `install.bat` file is located.

8. Type ‘install.bat” and press Enter.

Performing the installation on 64 bit OS

3. Open the file `Agent\wcsetup.ins` and update “LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows”.

4. Execute `installx64.bat` (If UAC is enabled, see [Performing the installation on Vista/2k8/Win7 when UAC is enabled](#)).
EventTracker 8.0

7. Download MSI package (e.g. AgentMSI_80.zip for v8.x) from the location provided by Prism Microsystems Support team.

The details about other versions are mentioned in table below. Refer Table 1.

8. Extract AgentMSI_80.zip to AgentMSI_8.0/.

9. Fill the necessary details in ‘Agent.ini’ configuration file (refer Table 2 on how to specify the parameters).

```
<table>
<thead>
<tr>
<th>EventTracker Agent Version</th>
<th>Zip file name</th>
<th>Executable file</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>7.1</td>
<td>AgentMSI_71.zip</td>
<td>etwAgent71.exe</td>
</tr>
<tr>
<td>7.2</td>
<td>AgentMSI_72.zip</td>
<td>etwAgent72.exe</td>
</tr>
<tr>
<td>7.3</td>
<td>AgentMSI_73.zip</td>
<td>etwAgent73.exe</td>
</tr>
<tr>
<td>7.4</td>
<td>AgentMSI_74.zip</td>
<td>etwAgent74.exe</td>
</tr>
<tr>
<td>7.5</td>
<td>AgentMSI_75.zip</td>
<td>etwAgent75.exe</td>
</tr>
<tr>
<td>7.6</td>
<td>AgentMSI_76.zip</td>
<td>etwAgent76.exe</td>
</tr>
<tr>
<td>8.0</td>
<td>AgentMSI_80.zip</td>
<td>etwAgent80.exe</td>
</tr>
</tbody>
</table>
```

Table 1
Deploy through Command Line

9. To launch command line, click the Start button, and then click Run.

10. In Run dialog box, type ‘CMD’, and then click the ‘Ok’ button.

11. Change directory to AgentMSI_8x.

12. Type ‘EventTrackerAgent.msi /qn’ command, and then click the Enter button.

NOTE:

- For Windows 8/8.1 and Windows 2012 operating system, .Net 3.5 will be enabled using a batch file provided in MSI package.
- All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently. If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
- If agent.ini file does not contain any parameters, and etaconfig.ini file is also present in the same folder, then silent installation will not be successful.

Deploy through User Interface

NOTE:


21. Click etwAgent.exe file for v8.0.

InstallShield Wizard pop up window appears on the screen.
The executable files for other versions are mentioned in Table 1.

22. Click the Next > button to start with installation.
23. Read the License Agreement, and then select the option 'I accept the terms in the license agreement'.
24. Click the **Next >** button.

25. In **Custom Setup**, select **EventTracker Windows Agent** and **Change Audit Agent** based on the requirement.

Refer Figure 6.
Click icon to select the installation options:

- **This feature will be installed on local hard drive**
- **This feature, and all subfeatures, will be installed on local hard drive**
- **This feature will not be available**

**Figure 29**

- Select **This feature will be installed on local hard drive** option to install only agent and not sub features.

**OR**

- Select **This feature, and all subfeatures, will be installed on local hard drive** option to install agent as well as its sub features.

**OR**

- Select the **This feature will not be available** option, if you do not wish to install the agent.
26. Click the **Change** button to change the installation path of the agent and then click the **Next >** button.

![EventTrackerAgent 8.0](image)

Figure 30

27. In the **Event destination** pane, there are two methods to install EventTracker and Change Audit agents:

- **Procedure to install with Agent.ini file**
- **Procedure to install with Agent.ini and etaconfig.ini files**

28. For Windows 8/8.1 and windows 2012 operating systems, .Net 3.5 will be enabled by using a batch file provided in MSI package in the same window.
NOTE:

- If the batch file asks the user to restart the system, select **No** or else after restarting, the user has to follow the above installation steps again.
- It is recommended to restart the system once all the MSI components get installed.
Procedure to install with Agent.ini file

i) Enter EventTracker Manager: (Ex. Win2k3x64), Port number: (Ex. 14505 to 14580).

j) Select Deploy SCAP/Deploy WINSCP option as per the requirement.

k) Enter License Server: (Ex. Win2k3x64), Port number: (Ex. 14503) and Change Audit Manager: (Ex. Win2k3x64).

l) Click the Next > button.

Refer Figure 10.

![EventTracker Agent Configuration](image)

Figure 33: Event Destination

NOTE:

If the agent.ini file has the proper inputs like manager name/port/license server etc., the application reads the information from the file automatically and displays the same in UI. There is no need to enter the values, provided if any change is required.
Procedure to install with Agent.ini and etaconfig.ini files

g) To achieve this, first copy ‘etaconfig.ini’ file from”<INSTALLDIR>\EventTracker\Agent“ folder to the same directory/folder where setup resides.

h) In Event destination pane, select Deploy SCAP / Deploy WINSCP option as per the requirement.

i) Enter Change Audit Manager: (Ex. Win2k3x64) details and then click the Next > button.

NOTE:

- If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
- Also, if the user doesn’t select SCAP or WINSCP, the agent will be installed with both the features.
29. In this last step of the installation process, check the **Install default Remedial action EXEs on this machine** option, and then click the **Install** button.

![Image of EventTrackerAgent 8.0 installation window](image)

**Figure 35**

**NOTE:**

To select **Install default Remedial action EXEs on this machine** option is not mandatory. If you do not wish to enable remedial action then do not select the option. Directly click the **Install** button.

30. In **Basic Configuration** dialog box, check the configuration options to apply to the manager system, and then click the **OK** button.

**NOTE:**

The **Basic Configuration** dialog box does not display if installation is carried out via **etaconfig.ini** file.
EventTracker Agent Deployment

NOTE:

If the deployed agent machine is not able to connect to the License Server, then the Basic Configuration window will come as blank, as displayed in the below figure:

![Basic Configuration Window](image)

**Figure 36: Basic Configuration**

EventTracker includes several important features. You can customize EventTracker by enabling/disabling the above list of available features.

**NOTE:**

If the deployed agent machine is not able to connect to the License Server, then the Basic Configuration window will come as blank, as displayed in the below figure:
31. Click the **Finish** button to complete the installation process.
Deploy through Group Policy

Before you Begin

7. Modify Agent.ini and change EM (ENTERPRISE_MANAGER), CM (Change Audit manager), INSTALLDIR (EventTracker Agent install directory) EP (ENTERPRISE_PORT), LS (License server name/ IP Address where the digital certificate is installed), and LP (License server port number) value appropriately.

<table>
<thead>
<tr>
<th>Configuration Settings</th>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>[INSTALL_PATH]</td>
<td>[INSTALL_PATH]</td>
</tr>
<tr>
<td>INSTALLDIR=&lt;Installation directory if agent need to be installed in other than default path&gt;</td>
<td>INSTALLDIR=</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[ENTERPRISE_MANAGER]</td>
<td>[ENTERPRISE_MANAGER]</td>
</tr>
<tr>
<td>EM=&lt;EventTracker Manager Hostname or IP Address&gt;</td>
<td>EM=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[ENTERPRISE_PORT]</td>
<td>[ENTERPRISE_PORT]</td>
</tr>
<tr>
<td>EP=&lt;EventTracker Enterprise Port number&gt;</td>
<td>EP=14580</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[CHANGEAUDIT_MANAGER]</td>
<td>[CHANGEAUDIT_MANAGER]</td>
</tr>
<tr>
<td>CM=&lt;Change Audit Manager Hostname or IP Address&gt;</td>
<td>CM=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[REMEDIAL_ACTIONS]</td>
<td>[REMEDIAL_ACTIONS]</td>
</tr>
<tr>
<td>IR=1</td>
<td>IR=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[LICENSE_SERVER]</td>
<td>[LICENSE_SERVER]</td>
</tr>
<tr>
<td>LS=&lt;The server name/ IP Address where the digital certificate is installed&gt;</td>
<td>LS=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>[LICENSE_SERVER_PORT]</td>
<td>[LICENSE_SERVER_PORT]</td>
</tr>
<tr>
<td>LP=&lt;License server port number&gt;</td>
<td>LP=14503</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>Deploy SCAP components</td>
<td>Deploy SCAP components</td>
</tr>
<tr>
<td>[DEPLOY_SCAP]</td>
<td>[DEPLOY_SCAP]</td>
</tr>
<tr>
<td>DS= ‘1’ or ‘0’</td>
<td>DS=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>Deploy WINSCP components</td>
<td>Deploy WINSCP components</td>
</tr>
<tr>
<td>[DEPLOY_WINSCP]</td>
<td>[DEPLOY_WINSCP]</td>
</tr>
<tr>
<td>DW= ‘1’ or ‘0’</td>
<td>DW=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
</tbody>
</table>

Table 2
8. Create a network share on server and allow **Domain Computers** to have at least **READ** access permission.

9. Copy the **AgentMSI_8x** folder to the network share, which is created in previous step.

Network share folder should have the below files.

![Figure 37](image)

**Acronyms Used:**

- **INSTALLDIR**: If this parameter is left blank, the files will be installed in the default location i.e. `%ProgramFiles%\Prism Microsystems`.

- Else you can specify the path where you wish to install the files.

- **EM**: If this parameter is left blank, Enterprise manager won’t be installed.

- **EP**: If this parameter is left blank, the installer will assume the default port.

- **CM**: If this parameter is left blank, Change Audit manager won’t be installed.

- **IR**: If 1 then remedial actions are installed, if 0 then remedial actions are not installed. If this parameter is left blank, the installer takes a default value as “1”.

- **LS**: The system name/ IP Address where the digital certificate is installed. If this parameter is left blank, the value will be read from EM (i.e. License server name will be the same as Enterprise manager)

- **LP**: If this parameter is left blank, the default port (i.e. 14503) will be assumed by the installer.
• **DS:** Deploy SCAP components. If the value is empty, then SCAP components will not be installed. If the value is ‘0’ or ‘1’, then SCAP components will be installed.

• **DW:** Deploy WINSCP components. If the value is empty then WINSCP components will not be installed. If the value is ‘0’ or ‘1’, then WINSCP components will be installed.

**NOTE:**

• All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently.

• It is mandatory to specify either Enterprise Manager name or Change Audit Manager name.

• If user wish to install EventTracker Agent then Enterprise Manager Name (EM) is mandatory.

• If user wish to install Change Audit Agent then Change Audit Manager Name (CM) is mandatory.

• **Remedial Actions** are scripts or EXEs that can be launched at either the Agent or Manager Side, in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder.

• **Microsoft XML Core Services (MSXML)** is installed along with the MSI Agent Installer setup for 32-bit and 64-bit machines respectively.

• The **Microsoft Visual C++ 2008 Redistributable Package (x86)** which installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ is also installed along with the MSI Agent Installer setup.

• Before deploying the Agent, make sure that the Agent system(s) and domain controller are synchronized.
Launch Group Policy Management Console

5. Select the **Start** button, select **Settings**, and then select **Control Panel**.
6. Select **Administrative Tools**, and then select **Group Policy Management**.

![Group Policy Management Console](image)
Create the Group Policy Object in Active Directory for Software Deployment

Follow the steps given below to create the new ‘Group Policy Object’ using the ‘Group Policy Management’ Snap-in,

43. In the **Group Policy Management** pane, expand **Domains** node, and then expand domain system node.

44. Right click **Group Policy Objects**, and then click **New**.

![Figure 18: Create Group Policy Object](image)

45. Enter a name for this new GPO (Ex. AgentMSI GPO) and then click the **OK** button.

![New GPO](image)
46. Click the name of newly created GPO. In this case, ‘AgentMSI GPO’.

G. In the Security Filtering pane, click the Add button to apply GPO settings to the domain computers group (or ensure the authenticated users group is listed).

H. In the Enter the object name to select field, type the object name or a part of the object name, and then click the Check Names button to select the object name.
I. Click the **OK** button.

47. Right click the newly created GPO, and then click **Edit**.

**Group Policy Object Editor** window will be opened.

E. Expand the **Computer Configuration**, and open **Software Settings**.

F. Right-click **Software Installation**, select **New**, and then select **Package**.
Open window displays.

E. Locate the UNC path of the server share where the MSI installer file is located (\Server\Share\AgentMSI_8x\).

F. Select the MSI installer file **EventTrackerAgent.msi**, and then click **Open**.

EventTracker displays 'Deploy Software' dialog box. Refer Figure 25.
48. Select **Assigned**, and then click **OK**.

You have now created and assigned the **Package Object**.

49. Right-click on the **Package Object**, and then select **Properties**.

50. Click the **Security** tab; select the **Add** button to add **Domain Computers** to provide security permissions.

Refer Figure 26.
51. Select the **Advanced** button, select **Find Now**.
Refer Figure 27.

52. Select Domain Computers from Search results, and then select **OK** button.

53. Select the **OK** button.
54. In EventTrackerAgent Properties pane, select Read and Write permissions. Select the Advanced button.

Refer Figure 29.

![EventTrackerAgent Properties](image)

**NOTE:**
Ensure Domain Computers has the Read and Write rights.

55. Select Domain Computers, and then click Edit.

Refer Figure 30.
Check the List Contents, Read All Properties, and Read Permissions options, if not selected. Select the OK button.

Refer Figure 30.

Select the Apply button and then select the OK button.

In Group Policy Management pane, right click the domain system name, and then select New Organizational Unit (OU).

A New Organizational Unit has to be created. Refer Figure 31.
59. Enter **New Organizational Unit** name.
   For example: Group Policy.
60. Right click newly created OU, and then click **Link an Existing GPO**.
   Refer Figure 32.
61. In the **Select GPO** dialog box, select the appropriate **domain name** and newly created **Group Policy Object**, and then click the **OK** button.

62. Close the **Group Policy window**.

   The **MSI package** has now been defined and is ready for the deployment.

63. Force replication to all other domain controllers.

**NOTE:**

EventTracker and Change Audit Agents will be installed once the target machines are restarted.

If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.

**Verify Installation**

Events will be sent to the target systems (i.e. “Manager” systems) upon successful deployment of EventTracker/ Change Audit agents. The name of the deployed agent along with their version number will appear in the System manager screen. On Target systems, following events will be generated in System Event Log:

**On Win XP, Win 2003 server operating systems**

On successful Agent deployment:

**Example 1:**

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Source</td>
<td>Application Management</td>
</tr>
<tr>
<td>Event Category</td>
<td>None</td>
</tr>
<tr>
<td>Event ID</td>
<td>301</td>
</tr>
<tr>
<td>User</td>
<td>NT AUTHORITY\SYSTEM</td>
</tr>
<tr>
<td>Computer</td>
<td>ESXWINXPVM8</td>
</tr>
<tr>
<td>Description</td>
<td>The assignment of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.</td>
</tr>
</tbody>
</table>

**Example 2:**
EventTracker Agent Deployment

Event Type : Information
Event Source : Application Management
Event Category: None
Event ID : 302
User : NT AUTHORITY\SYSTEM
Computer : ESXWINXPVM8
Description : The install of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

On Failed Agent deployment:

Event Type : Warning
Event Source : Application Management
Event Category: None
Event ID : 102
User : NT AUTHORITY\SYSTEM
Computer : ESXWINXPVM8
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.


On Successful Agent Deployment:

Example 1:

Log Name : System
Source : Application Management Group Policy
Event ID : 301
Task Category : None
Level : Information
Keywords : Classic
EventTracker Agent Deployment

User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The assignment of application EventTrackerAgent from policy Software Deployment policy succeeded.

Example 2:
Log Name : System
Source : Application Management Group Policy
Event ID : 302
Task Category : None
Level : Information
Keywords : Classic
User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy succeeded.

On Failed Agent Deployment:
Log Name : System
Source : Application Management Group Policy
Event ID : 102
Task Category : None
Level : Error
Keywords : Classic
User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.

Limitation for Group Policy Installation

- Retain configuration does not work via Group policy
- Upgrade agents is not supported via Group policy
- Modification features are not supported via Group policy
- Command line or silent installation doesn't support retain, upgrade and modify functions
- If EventTracker and Change Audit agent is installed via group policy then it is not possible to configure group policy to uninstall Change Audit or EventTracker agent only. While uninstalling both EventTracker and Change Audit agent will be uninstalled.

How to deploy agent via Agent MSI in Server Core Machine?

15. Login to the server core system.

16. Copy the MSI package in the drive of server core machine. Make sure that the user has permission to the system.

17. Extract AgentMSI_80.zip to AgentMSI_80/.

18. Open Task Manager by pressing the key combinations Ctrl + Shift+ Esc.

20. To open Command prompt, type **CMD** in the **Create New Task** Screen.

![Figure 33](image)

21. The Command Prompt Screen will be displayed.

![Figure 34](image)
Deploy through Command Line

7. To locate the MSI package, type the following commands:

   g. Exit from the System 32 folder by typing the command `Cd\`

   h. Change the directory to Agentmsi_80 by entering the command `Cd Agentmsi_80`.

   i. Now, open the Agent.ini file by typing `Agent.ini`.

   ![Figure 35](image)

   The Agent.ini file will be displayed.

8. Fill the necessary details in 'Agent.ini' configuration file.
9. Type `EventTrackerAgent.msi /qn` command, and then click the Enter button.

For Windows 8 /8.1 and Windows 2012 operating systems, .Net 3.5 will be enabled by using a batch file provided in MSI package in the same window.
Deploy through User Interface

9. Type `dir` to list the files that are available in the `Agentmsi_80` folder.

   The files inside the directory are listed

10. Execute **etwAgent.exe** file by typing **etwAgent.exe**.

11. The EventTracker 8.0 InstallShield Wizard will get started.
12. To continue with the installation steps, please refer to Deploy through User Interface.

Uninstall EventTracker Agent

17. Open Task Manager by pressing the key combinations Ctrl + Shift+ Esc.

18. Click Run New Task from File Menu.
19. Type `regedit` in the **Create New Task** Screen.

The **Registry Editor** screen will be displayed.
Go to the following location to find the registry keys:

\Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\n
Figure 43

20. Traverse through all the registry keys until you find:
   - DisplayName: EventTrackerAgent
   - Installsource: AgentMSI_80
21. Copy the key.

22. Open the Command Prompt and type `MsiExec.exe/uninstall` followed by the key.
23. Select **Yes** to confirm.

![Figure 46](image.png)
24. You will be asked whether to retain agent configuration settings.

Click **Yes** if you wish to retain agent Configuration settings or else click **No**.

**NOTE**

In case you get the below message during the uninstall process, then the EventTracker and Change audit process has to be killed from task manager.
How to launch EventTracker agent?

5. Type `dir` to list the files that are available in the Agent folder.
   
The files inside the directory are listed.

6. Type `etaconfig.exe` and press Enter to open EventTracker Agent Configuration.

   ![EventTracker Agent Configuration](image)
How to launch Change Audit agent

7. Change directory to the path where WcWindows folder is located.

8. Type dir to list the files that are available in the WcWindows folder.

9. Type WcWindows.exe and press Enter to open EventTracker Change Audit Agent.

The EventTracker change audit agent is launched.
Manual Agent install V8.0 [Batch File Install]

Installing EventTracker Agent

NOTE

The agent installation procedure is applicable only for EventTracker V 8.0 users.

Preparing the files for manual agent installation

13. Extract the zip file in the root directory of install drive.

14. Replace Agent\AliTemp\etaconfig.ini with your copy of etaconfig.ini.
   OR
   Specify the manager details in Agent\AliTemp\etaconfig.ini

15. Specify the license server details in Agent\etsetup.ins. Open the file Agent\etsetup.ins in notepad and replace "LicServ_Name=" with "LicServ_Name=<LicenseServerName>". Substitute the text "<LicenseServerName>" with the name/IP of manager system.

16. If program files shortcut menu is not required, then open the file Agent\etsetup.ins in notepad and replace "PgmMenuShortCutReq=1" with "PgmMenuShortCutReq=0".

17. If you do not want to install SCAP components on target system, then open the file Agent\etsetup.ins in notepad and replace "ETADeploySCAP=1" with "ETADeploySCAP=0".

18. If you do not want to install WinSCP components on target system, then open the file Agent\etsetup.ins in notepad and replace "ETADeployWinSCP=1" with "ETADeployWinSCP=0".

The default etaconfig.ini available with this installer will not have a manager, license server configured, and File transfer, and Configuration assessment are disabled. If the default copy is not replaced, then please configure Manager and required settings by opening Programs-> EventTracker-> Agent Config (Agent Configuration GUI) or by running "etaconfig.exe" from installation path.
Performing the installation on XP/2K3

5. Execute install.bat.

Performing the installation on Vista/2K8/Win7 when UAC is enabled

9. Go to Start -> All Programs -> Accessories.

10. Right click on **Command Prompt** and select **Run as administrator** to open the command prompt as administrator.

11. In the command prompt change the directory to the path where install.bat file is located.

12. Type "install.bat" and press enter.

Performing the installation on Vista/2K8/Win7 (64 bit OS)

3. Open the file Agent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

6. Execute installx64.bat bat (If UAC is enabled, see Performing the installation on Win8 (32 bit OS).

5. Performing the installation on Win8 (32 bit OS)

12. If you're using a keyboard with Windows 8, you can open an elevated Command Prompt from the Power User Menu. Just press the "WINDOWS" and "X" keys together and then click on "Command Prompt (Admin)".

13. Click "Yes" to the User Account Control message that appears.

14. In the command prompt, change the directory to the path where install.bat file is located.

15. Type "install.bat" and press enter.

**IMPORTANT NOTE:** Prior to installing agent on Win8 (32bit), user has to apply all important Windows updates which are related to .NET Framework 3.5.
Performing the installation on Win8/8.1/2012/10 (64 bit OS)

3. Open the file Agent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

4. Execute installx64.bat (If UAC is enabled, see Performing the installation on Win8 (32 bit OS).

IMPORTANT NOTE: Prior to installing agent on Win8/8.1/2012 (64 bit), user has to apply all important Windows updates which are related to .NET Framework 3.5.

Preparing the files for manual agent installation (EventTracker Change Audit Agent)

11. Extract the zip file in the root directory of install drive.

12. Replace Agent\AITemp\ wcw.ini with your copy of wcw.ini.

13. Open the file Agent\wcsetup.ins in notepad and replace “Server=0” with “Server=<ManagerName>”. Substitute the text “<ManagerName>” with the name of manager system.

14. If program files shortcut menu is not required, then open the file Agent\ wcsetup.ins in notepad and replace “PgmMenuShortCutReq=1” with “PgmMenuShortCutReq=0”.

15. Specify the license server details in Agent\wcsetup.ins. Open the file Agent\wcsetup.ins in notepad and replace “LicServ_Name=0” with “LicServ_Name=<LicenseServerName>”. Substitute the text “<LicenseServerName>” with the name/IP of manager system.

Performing the installation on XP/2K3

3. Execute install.bat.

Performing the installation on Vista/2k8/Win7 when UAC is enabled

9. Go to Start -> All Programs -> Accessories.

10. Right click ‘Command Prompt’ and select ‘Run as administrator” to open the command prompt as administrator.
11. In the command prompt change the directory to the path where `install.bat` file is located.

12. Type `install.bat` and press Enter.

Performing the installation on 64 bit OS

5. Open the file `Agent\wcsetup.ins` and update "LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows".

6. Execute `installx64.bat` (If UAC is enabled, see Performing the installation on Vista/2k8/Win7 when UAC is enabled).

EventTracker 7.6X

1. Download MSI package (e.g. `AgentMSI_7x.zip` for v7.x where x is the version number 1/2/3/4/5) from the location provided by Prism Microsystems Support team.

   The details about other versions are mentioned in table below. Refer Table 1.

2. Extract `AgentMSI_7x.zip` to `AgentMSI_7x`.

3. Fill the necessary details in `Agent.ini` configuration file (refer Table 2 on how to specify the parameters).

<table>
<thead>
<tr>
<th>EventTracker Agent Version</th>
<th>Zip file name</th>
<th>Executable file</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>7.1</td>
<td><code>AgentMSI_71.zip</code></td>
<td><code>etwAgent71.exe</code></td>
</tr>
<tr>
<td>7.2</td>
<td><code>AgentMSI_72.zip</code></td>
<td><code>etwAgent72.exe</code></td>
</tr>
</tbody>
</table>
## Deploy through Command Line

To launch command line, click the **Start** button, and then click **Run**.

1. In **Run** dialog box, type ‘**CMD**’, and then click the ‘**Ok**’ button.
2. Change directory to **AgentMSI_7x** (where x is the version number 1/2/3/4/5).
3. Type ‘**EventTrackerAgent.msi /qn**’ command, and then click the **Enter** button.

### NOTE:
- On Vista, Win 7, Win 8, Win 2008, 2008 R2, Win 2012 and Win 2012 R2 (v7.6 Build 21 and above) operating systems, the MSI Installer executable should be run with ‘Administrative’ privileges.
- For Windows 8/8.1 and Windows 2012 operating system, .Net 3.5 will be enabled using a batch file provided in MSI package.
- All the parameters will be read from the "**Agent.ini**" configuration settings file, when the installer is running silently. If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
- If agent.ini file does not contain any parameters, and etaconfig.ini file is also present in the same folder, then silent installation will not be successful.

## Deploy through User Interface

### NOTE:

32. Click **etwAgent.exe** file for v7.6.

**InstallShield Wizard** pop up window appears on the screen.
The executable files for other versions are mentioned in Table 3.

33. Click the **Next >** button to start with installation.
Figure 54

34. Read the License Agreement, and then select the option 'I accept the terms in the license agreement'.
35. Click the **Next** button.

36. In **Custom Setup**, select **EventTracker Windows Agent** and **Change Audit Agent** based on the requirement.

Refer Figure 56.
Click on an icon in the list below to change how a feature is installed.

![Custom Setup](image)

- **Select 'This feature will be installed on local hard drive'** option to install only agent and not sub features.
- **Select 'This feature, and all subfeatures, will be installed on local hard drive'** option to install agent as well as its sub features.
- **Select the 'This feature will not be available'** option, if you do not wish to install the agent.

37. Click the **Change** button to change the installation path of the agent and then click the **Next >** button.
38. In the **Event destination** pane, there are two methods to install EventTracker and Change Audit agents:

- Procedure to install with Agent.ini file
- Procedure to install with Agent.ini and etaconfig.ini files

39. For Windows 8 /8.1 and windows 2012 operating systems, .Net 3.5 will be enabled by using a batch file provided in MSI package in the same window.
NOTE:

- If the batch file asks the user to restart the system, select **No** or else after restarting, the user has to follow the above installation steps again.
- It is recommended to restart the system once all the MSI components get installed.
Procedure to install with Agent.ini file

m) Enter **EventTracker Manager**: (Ex. Win2k3x64), **Port number**: (Ex. 14505 to 14595).

n) Select **Deploy SCAP/Deploy WINSCP** option as per the requirement.

o) Enter **License Server**: (Ex. Win2k3x64), **Port number**: (Ex. 14503) and **Change Audit Manager**: (Ex. Win2k3x64).

p) Click the **Next >** button.

Refer Figure 59.

![EventTrackerAgent 7.6](image)

**NOTE:**

If the agent.ini file has the proper inputs like manager name/port/license server etc., the application reads the information from the file automatically and displays the same in UI. There is no need to enter the values, provided if any change is required.
Procedure to install with Agent.ini and etaconfig.ini files

j) To achieve this, first copy ‘etaconfig.ini’ file from “<INSTALLDIR>\EventTracker\Agent” folder to the same directory/folder where setup resides.

k) In Event destination pane, select Deploy SCAP / Deploy WINSCP option as per the requirement.

l) Enter Change Audit Manager: (Ex. Win2k3x64) details and then click the Next > button.

![Figure 62](image)

NOTE:

- If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
- Also, if the user doesn’t select SCAP or WINSCP, the agent will be installed with both the features (v7.6x).
40. In this last step of the installation process, check the 'Install default Remedial action EXEs on this machine' option, and then click the Install button.

![Figure 63](image)

**NOTE:**

To select 'Install default Remedial action EXEs on this machine' option is not mandatory. If you do not wish to enable remedial action then do not select the option. Directly click the Install button.

41. In Basic Configuration dialog box, check the configuration options to apply to the manager system, and then click the OK button.

**NOTE:**

The Basic Configuration dialog box does not display if installation is carried out via etaconfig.ini file.
EventTracker Agent Deployment

Figure 64: Basic Configuration

NOTE:

If the deployed agent machine is not able to connect to the License Server, then the Basic Configuration window will come as blank, as displayed in the below figure:
42. Click the **Finish** button to complete the installation process.
The InstallShield Wizard has successfully installed EventTrackerAgent. Click Finish to exit the wizard.

Figure 66
Deploy through Group Policy

Before you Begin

10. Modify `Agent.ini` and change **EM** (ENTERPRISE_MANAGER), **CM** (Change Audit manager), **INSTALLDIR** (EventTracker Agent install directory) **EP** (ENTERPRISE_PORT), **LS** (License server name/ IP Address where the digital certificate is installed), and **LP** (License server port number) value appropriately.

<table>
<thead>
<tr>
<th>Configuration Settings</th>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>[INSTALL_PATH] INSTALLDIR=&lt;Installation directory if agent need to be installed in other than default path&gt; [END] [ENTERPRISE_MANAGER] EM=&lt;EventTracker Manager Hostname or IP Address&gt; [END] [ENTERPRISE_PORT] EP=&lt;EventTracker Enterprise Port number&gt; [END] [CHANGEAUDIT_MANAGER] CM=&lt;Change Audit Manager Hostname or IP Address&gt; [END] [REMEDIAL_ACTIONS] IR=1 [END] [LICENSE_SERVER] LS=&lt;The server name/ IP Address where the digital certificate is installed&gt; [END] [LICENSE_SERVER_PORT] LP=&lt;License server port number&gt; [END] Deploy SCAP components [DEPLOY_SCAP] DS= ‘1’ or ‘0’ [END] Deploy WINSCP components [DEPLOY_WINSCP] DW= ‘1’ or ‘0’ [END]</td>
<td>[INSTALL_PATH] INSTALLDIR= [END] [ENTERPRISE_MANAGER] EM=Win2k3x64 [END] [ENTERPRISE_PORT] EP=14580 [END] [CHANGEAUDIT_MANAGER] CM=Win2k3x64 [END] [REMEDIAL_ACTIONS] IR=1 [END] [LICENSE_SERVER] LS=Win2k3x64 [END] [LICENSE_SERVER_PORT] LP=14503 [END] Deploy SCAP components [DEPLOY_SCAP] DS=1 [END] Deploy WINSCP components [DEPLOY_WINSCP] DW=1 [END]</td>
</tr>
</tbody>
</table>

Table 4
11. Create a network share on server and allow **Domain Computers** to have at least **READ** access permission.

12. Copy the **AgentMSI_7x** folder to the network share, which is created in previous step.

   Network share folder should have the below files.

   ![AgentMSI_7x folder contents](image)

   **Figure 67**

**Acronyms Used:**

- **INSTALLDIR:** If this parameter is left blank, the files will be installed in the default location i.e. %ProgramFiles%\Prism Microsystems.

- Else you can specify the path where you wish to install the files.

- **EM:** If this parameter is left blank, Enterprise manager won’t be installed.

- **EP:** If this parameter is left blank, the installer will assume the default port.

- **CM:** If this parameter is left blank, Change Audit manager won’t be installed.

- **IR:** If 1 then remedial actions are installed, if 0 then remedial actions are not installed. If this parameter is left blank, the installer takes a default value as “1”.

- **LS:** The system name/ IP Address where the digital certificate is installed. If this parameter is left blank, the value will be read from EM (i.e. License server name will be the same as Enterprise manager)

- **LP:** If this parameter is left blank, the default port (i.e. 14503) will be assumed by the installer.
• **DS:** Deploy SCAP components. If the value is empty, then SCAP components will not be installed. If the value is ‘0’ or ‘1’, then SCAP components will be installed.

• **DW:** Deploy WINSCP components. If the value is empty then WINSCP components will not be installed. If the value is ‘0’ or ‘1’, then WINSCP components will be installed.

**NOTE:**

• All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently.

• It is mandatory to specify either Enterprise Manager name or Change Audit Manager name.

• If user wish to install EventTracker Agent then Enterprise Manager Name (EM) is mandatory.

• If user wish to install Change Audit Agent then Change Audit Manager Name (CM) is mandatory.

• **Remedial Actions** are scripts or EXEs that can be launched at either the Agent or Manager Side, in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder.

• **Microsoft XML Core Services (MSXML)** is installed along with the MSI Agent Installer setup for 32-bit and 64-bit machines respectively.

• The Microsoft Visual C++ 2008 Redistributable Package (x86) which installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ is also installed along with the MSI Agent Installer setup.

• Before deploying the Agent, make sure that the Agent system(s) and domain controller are synchronized.
Launch Group Policy Management Console

7. Select the **Start** button, select **Settings**, and then select **Control Panel**.
8. Select **Administrative Tools**, and then select **Group Policy Management**.
Create the Group Policy Object in Active Directory for Software Deployment

Follow the steps given below to create the new ‘Group Policy Object’ using the ‘Group Policy Management’ Snap-in,

64. In the Group Policy Management pane, expand Domains node, and then expand domain system node.

65. Right click Group Policy Objects, and then click New.

66. Enter a name for this new GPO (Ex. AgentMSI GPO) and then click the OK button.
Figure 70: New GPO

67. Click the name of newly created GPO. In this case, ‘AgentMSI GPO’.

Figure 71

J. In the **Security Filtering** pane, click the **Add** button to apply GPO settings to the domain computers group (or ensure the authenticated users group is listed).

K. In the **Enter the object name to select** field, type the object name or a part of the object name, and then click the **Check Names** button to select the object name.
L. Click the **OK** button.

68. Right click the newly created GPO, and then click **Edit**.

**Group Policy Object Editor** window will be opened.

G. Expand the **Computer Configuration**, and open **Software Settings**.

H. Right-click **Software Installation**, select **New**, and then select **Package**.
Figure 74: Software installation, create new package

Open window displays.

G. Locate the UNC path of the server share where the MSI installer file is located (\Server\Share\AgentMSI_7x) where x is version number 1/2/3/4/5).

H. Select the MSI installer file EventTrackerAgent.msi, and then click Open.

EventTracker displays 'Deploy Software' dialog box. Refer Figure 76.
69. Select **Assigned**, and then click **OK**.

You have now created and assigned the **Package Object**.

70. Right-click on the **Package Object**, and then select **Properties**.

71. Click the **Security** tab; select the **Add** button to add **Domain Computers** to provide security permissions.

Refer Figure 77.
72. Select the **Advanced** button, select **Find Now**.
Refer Figure 78.

![Select Users, Computers, or Groups](image)

73. Select Domain Computers from Search results, and then select OK button.

![Select Users, Computers, or Groups](image)

74. Select the **OK** button.
75. In EventTrackerAgent Properties pane, select Read and Write permissions. Select the Advanced button.
   Refer Figure 80.

![EventTrackerAgent Properties](image)

**NOTE:**
Ensure Domain Computers has the Read and Write rights.

76. Select Domain Computers, and then click Edit.

Refer Figure 81.
77. Check the List Contents, Read All Properties, and Read Permissions options, if not selected. Select the OK button.

Refer Figure 81.

78. Select the Apply button and then select the OK button.

79. In Group Policy Management pane, right click the domain system name, and then select New Organizational Unit (OU).

A New Organizational Unit has to be created. Refer Figure 82.
80. Enter **New Organizational Unit** name.

For example: Group Policy.

81. Right click newly created OU, and then click **Link an Existing GPO**.

Refer Figure 83.
82. In the Select GPO dialog box, select the appropriate domain name and newly created Group Policy Object, and then click the OK button.

83. Close the Group Policy window.

The MSI package has now been defined and is ready for the deployment.

84. Force replication to all other domain controllers.

NOTE:

EventTracker and Change Audit Agents will be installed once the target machines are restarted.

If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
Verify Installation

Events will be sent to the target systems (i.e. "Manager" systems) upon successful deployment of EventTracker/Change Audit agents. The name of the deployed agent along with their version number will appear in the System manager screen. On Target systems, following events will be generated in System Event Log:

On Win XP, Win 2003 server operating systems

On successful Agent deployment:

**Example 1:**

- Event Type: Information
- Event Source: Application Management
- Event Category: None
- Event ID: 301
- User: NT AUTHORITY\SYSTEM
- Computer: ESXWINXPVM8
- Description: The assignment of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

**Example 2:**

- Event Type: Information
- Event Source: Application Management
- Event Category: None
- Event ID: 302
- User: NT AUTHORITY\SYSTEM
- Computer: ESXWINXPVM8
- Description: The install of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

On Failed Agent deployment:

- Event Type: Warning
Event Source : Application Management
Event Category: None
Event ID : 102
User : NT AUTHORITY\SYSTEM
Computer : ESXWINXPVM8
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.


On Successful Agent Deployment:

Example 1:
Log Name : System
Source : Application Management Group Policy
Event ID : 301
Task Category : None
Level : Information
Keywords : Classic
User : SYSTEM
Computer : Esxwin2k8r2vm3.Toons.local
Description : The assignment of application EventTrackerAgent from policy Software Deployment policy succeeded.

Example 2:
Log Name : System
Source : Application Management Group Policy
Event ID : 302
Task Category : None
Level : Information
Keywords : Classic
User : SYSTEM
Computer : Esxwin2k8r2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software
Deployment policy succeeded.

On Failed Agent Deployment:

Log Name : System
Source : Application Management Group Policy
Event ID : 102
Task Category : None
Level : Error
Keywords : Classic
User : SYSTEM
Computer : Esxwin2k8r2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software
Deployment policy failed.

Limitation for Group Policy Installation

- Retain configuration does not work via Group policy
- Upgrade agents is not supported via Group policy
- Modification features are not supported via Group policy
- Command line or silent installation doesn't support retain, upgrade and modify functions
- If EventTracker and Change Audit agent is installed via group policy then it is not possible
to configure group policy to uninstall Change Audit or EventTracker agent only. While
uninstalling both EventTracker and Change Audit agent will be uninstalled.
- GPO Deployment fails in Windows server 2012/R2 (Use command line installation for the
respective Operating System).
How to deploy agent via Agent MSI in Server Core Machine?

22. Login to the server core system.

23. Copy the MSI package in the drive of server core machine. Make sure that the user has permission to the system.

24. Extract AgentMSI_76.zip to AgentMSI_76/.

25. Open Task Manager by pressing the key combinations Ctrl + Shift + Esc.


27. To open Command prompt, type CMD in the Create New Task Screen.
28. The Command Prompt Screen will be displayed.

**Deploy through Command Line**

10. To locate the MSI package, type the following commands:

   j. Exit from the **System 32** folder by typing the command `Cd\`

   k. Change the directory to **Agentmsi_76** by entering the command `Cd Agentmsi_76`.

   l. Now, open the **Agent.ini** file by typing `Agent.ini`.
The **Agent.ini** file will be displayed.

11. Fill the necessary details in ‘**Agent.ini**’ configuration file.

![Figure 87](image)

12. Type ‘**EventTrackerAgent.msi /qn**’ command, and then click the **Enter** button.
For Windows 8 / 8.1 and Windows 2012 operating systems, .Net 3.5 will be enabled by using a batch file provided in MSI package in the same window.

**Deploy through User Interface**

13. Type `dir` to list the files that are available in the `Agentmsi_76` folder.

The files inside the directory are listed.

![Figure 90](image_url)

15. The EventTracker 7.6 InstallShield Wizard will get started.

![Figure 91](image_url)

16. To continue with the installation steps, please refer to [Deploy through User Interface](#).
Uninstall EventTracker Agent

25. Open **Task Manager** by pressing the key combinations **Ctrl + Shift + Esc**.

26. Click **Run New Task** from **File** Menu.

27. Type `regedit` in the Create New Task Screen.
The Registry Editor screen will be displayed.

Go to the following location to find the registry keys:

`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall`  

![Registry Editor Screen](image)

**Figure 94**

28. Traverse through all the registry keys until you find:
   - DisplayName: `EventTrackerAgent`
   - Installsource: `AgentMSI_76`
29. Copy the key.

30. Open the Command Prompt and type `MsiExec.exe/uninstall` followed by the key.
31. Select **Yes** to confirm.
32. You will be asked whether to retain agent configuration settings.

Click **Yes** if you wish to retain agent Configuration settings or else click **No**.

**NOTE**

In case you get the below message during the uninstall process, then the EventTracker and Change audit process has to be killed from task manager.
How to launch EventTracker agent?

7. Type `dir` to list the files that are available in the *Agent* folder.

The files inside the directory are listed.

8. Type `etaconfig.exe` and press Enter to open *EventTracker Agent Configuration*. 
How to launch Change Audit agent

10. Change directory to the path where WcWindows folder is located.

11. Type dir to list the files that are available in the WcWindows folder.

12. Type WcWindows.exe and press Enter to open EventTracker Change Audit Agent.

![The EventTracker change audit agent is launched.](image)

The EventTracker change audit agent is launched.
Manual Agent install V7.6 [Batch File Install]

Installing EventTracker Agent

NOTE

The agent installation procedure is applicable only for EventTracker V 7.6 users.

Preparing the files for manual agent installation

1. Extract the zip file in the root directory of install drive.
2. Replace `Agent\AITemp\etaconfig.ini` with your copy of `etaconfig.ini`.

OR

Specify the manager details in `Agent\AITemp\etaconfig.ini`

3. Specify the license server details in `Agent\etsetup.ins`. Open the file `Agent\etsetup.ins` in notepad and replace `LicServ_Name="` with `LicServ_Name=<LicenseServerName>`". Substitute the text `"<LicenseServerName>"` with the name/IP of manager system.

4. If program files shortcut menu is not required, then open the file `Agent\etsetup.ins` in notepad and replace `"PgmMenuShortCutReq=1"` with `"PgmMenuShortCutReq=0"`.

5. If you do not want to install SCAP components on target system, then open the file `Agent\etsetup.ins` in notepad and replace `"ETADeploySCAP=1"` with `"ETADeploySCAP=0"`.

6. If you do not want to install WinSCP components on target system, then open the file `Agent\etsetup.ins` in notepad and replace `"ETADeployWinSCP=1"` with `"ETADeployWinSCP=0"`.

The default `etaconfig.ini` available with this installer will not have a manager, license server configured, and File transfer, and Configuration assessment are disabled. If the default copy is not replaced, then please configure Manager and required settings by opening Programs-> EventTracker-> Agent Config (Agent Configuration GUI) or by running "etaconfig.exe" from installation path.
Performing the installation on XP/2K3

5. Execute install.bat.

Performing the installation on Vista/2k8/Win7 when UAC is enabled

1. Go to Start -> All Programs -> Accessories.
2. Right click 'Command Prompt' and select 'Run as administrator' to open the command prompt as administrator.
3. In the command prompt change the directory to the path where install.bat file is located.
4. Type install.bat and press Enter.

Performing the installation on Vista/2k8/Win7 (64 bit OS)

1. Open the file Agent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".
2. Execute installx64.bat (If UAC is enabled, see Performing the installation on Vista/2k8/Win7 when UAC is enabled).

Performing the installation on Win8 (32 bit OS)

1. If you're using a keyboard with Windows 8, you can open an elevated Command Prompt from the Power User Menu. Just press the ‘WINDOWS’ and ‘X’ keys together and then click ‘Command Prompt (Admin)’.
2. Click ‘Yes’ to the User Account Control message that appears.
3. In the command prompt, change the directory to the path where install.bat file is located.
4. Type ‘install.bat’ and press Enter.
Performing the installation on Win8/8.1/2012 (64 bit OS)

6. Open the file Agent\etsetup.ins and update "INSTALLPATH="\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

7. Execute installx64.bat (If UAC is enabled, see Performing the installation on Win8 (32 bit OS).

EventTracker Change Audit Agent installation (Manual):

Preparing the files for manual agent installation

1. Extract the zip file in the root directory of install drive.

2. Replace Agent\AlTemp\ wcw.ini with your copy of wcw.ini.

3. Open the file Agent\wcsetup.ins in notepad and replace ‘Server=0” with ‘Server=<ManagerName>“. Substitute the text ‘<ManagerName>“ with the name of manager system.

4. If shortcut menu is not required in Program Files, then open the file Agent\wcsetup.ins in notepad and replace ‘PgmMenuShortCutReq=1“ with ‘PgmMenuShortCutReq=0“.

5. Specify the license server details in Agent\wcsetup.ins. Open the file Agent\wcsetup.ins in notepad and replace ‘LicServ_Name=0” with ‘LicServ_Name=<LicenseServerName>“. Substitute the text ‘<LicenseServerName>“ with the name/IP of manager system.

Performing the installation on XP/2K3

4. Execute install.bat.

Performing the installation on Vista/2k8/Win7 when UAC is enabled

13. Go to Start -> All Programs -> Accessories.
14. Right click ‘Command Prompt’ and select ‘Run as administrator’ to open the command prompt as administrator.

15. In the command prompt change the directory to the path where install.bat file is located.

16. Type ‘install.bat’ and press Enter.

Performing the installation on 64 bit OS

7. Open the file Agent\wcsetup.ins and update "LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows".

8. Execute installx64.bat (If UAC is enabled, see Performing the installation on Vista/2k8/Win7 when UAC is enabled).
EventTracker 7.5X

1. Download MSI package (e.g. AgentMSI_7x.zip for v7.x where x is the version number 1/2/3/4/5) from the location provided by Prism Microsystems Support team.

   The details about other versions are mentioned in table below. Refer Table 3.

2. Extract AgentMSI_7x.zip to AgentMSI_7x.

3. Copy License certificate file to Extracted folder (AgentMSI_7x) and rename it to EventTracker.cer.

4. Fill the necessary details in ‘Agent.ini’ configuration file (refer Table 4 on how to specify the parameters).

5. The installer will look for the certificate file to be present in the same folder (Refer the highlighted file in the Figure 1) where the files are extracted. So, please copy the certificate file to AgentMSI_7x folder.
### Table 5

<table>
<thead>
<tr>
<th>EventTracker Agent Version</th>
<th>Zip file name</th>
<th>Executable file</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>7.1</td>
<td>AgentMSI_71.zip</td>
<td>etwAgent71.exe</td>
</tr>
<tr>
<td>7.2</td>
<td>AgentMSI_72.zip</td>
<td>etwAgent72.exe</td>
</tr>
<tr>
<td>7.3</td>
<td>AgentMSI_73.zip</td>
<td>etwAgent73.exe</td>
</tr>
<tr>
<td>7.4</td>
<td>AgentMSI_74.zip</td>
<td>etwAgent74.exe</td>
</tr>
<tr>
<td>7.5</td>
<td>AgentMSI_75.zip</td>
<td>etwAgent75.exe</td>
</tr>
</tbody>
</table>

#### Deploy through Command Line

1. To launch command line, click the **Start** button, and then click **Run**.
2. In **Run** dialog box, type ‘**CMD**’, and then click the ‘**Ok**’ button.
3. Change directory to **AgentMSI_7x** (where x is the version number 1/2/3/4/5).
4. Type ‘**EventTrackerAgent.msi /qn**’ command, and then click the **Enter** button.

**NOTE:**

- On Vista, Win 7, Win 8, Win 2008, 2008 R2, Win 2012 and Win 2012 R2 (v7.5 Build 29 and above) operating systems, the MSI Installer executable should be run with ‘Administrative’ privileges.

- All the parameters will be read from the "**Agent.ini**" configuration settings file, when the installer is running silently. If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.

- If agent.ini file does not contain any parameters, and etaconfig.ini file is also present in the same folder, then silent installation will not be successful.

- If you wish to place the certificate file in a different location, then please provide the full path along with the certificate name in the configuration settings file (i.e. DC = Digital Certificate full path along with the certificate name).
Deploy through User Interface

NOTE:

On Vista, Win 7, Win 8, Win 2008, Win 2008 R2, Win 2012 and Win 2012 R2 (v7.5 Build 29 and above) operating systems, the MSI Installer executable should be run with ‘Administrative’ privileges.

1. Click etwAgent75.exe file for v7.5.

   InstallShield Wizard pop up window appears on the screen.

   ![Figure 104](image)

   The executable files for other versions are mentioned in Table 5.

2. Click the Next > button to start with installation.
3. Read the License Agreement, and then select the option 'I accept the terms in the license agreement'.
4. Click the **Next >** button.

5. Browse and locate the certificate file.
6. Click the **Next >** button.

7. In **Custom Setup**, select **EventTracker Windows Agent** and **Change Audit Agent** based on the requirement.

   Refer Figure 108.
Click on an icon in the list below to change how a feature is installed.

- **EventTracker Windows Agent**
  - **Feature Description**: Install only the Windows Agent component.
  - **Install to**: C:\Program Files (x86)\Prism Microsystems\ (Change...)

- **Change Audit Agent**

Click icon to select the installation options:

- **This feature will be installed on local hard drive**
- **This feature, and all subfeatures, will be installed on local hard drive**
- **This feature will not be available**

8. Click the Change button to change the installation path of the agent and then click the Next > button.
9. In the Event destination pane, there are two methods to install EventTracker and Change Audit agents:

- Procedure to install with Agent.ini file
- Procedure to install with Agent.ini and etaconfig.ini files

Procedure to install with Agent.ini file

a) Enter EventTracker Manager: (Ex. Win2k3x64), Port number: (Ex. 14505 to 14595).

b) Select Deploy SCAP / Deploy WINSCP option as per the requirement.

c) Enter License Server: (Ex. Win2k3x64), Port number: (Ex. 14503) and Change Audit Manager: (Ex. Win2k3x64).

d) Click the Next > button.
Refer Figure 111.

**NOTE:**
If the agent.ini file has the proper inputs like manager name/port/license server etc., the application reads the information from the file automatically and displays the same in UI. There is no need to enter the values, provided if any change is required.

### Procedure to install with Agent.ini and etaconfig.ini files

- **a)** To achieve this, first copy 'etaconfig.ini' file from "<INSTALLDIR>\EventTracker\Agent" folder to the same directory/folder where setup resides.

- **b)** In Event destination pane, select **Deploy SCAP** / **Deploy WINSCP** option as per the requirement.
c) Enter **Change Audit Manager** (Ex. Win2k3x64) details and then click the **Next >** button.

![Image of EventTracker Agent Deployment](image.png)

**Figure 112**

**NOTE:**

If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.

10. In this last step of the installation process, check the **Install default Remedial action EXEs on this machine** option, and then click the **Install** button.
NOTE:

To select 'Install default Remedial action EXEs on this machine' option is not mandatory. If you do not wish to enable remedial action then do not select the option. Directly click the Install button.

11. In Basic Configuration dialog box, check the configuration options to apply to the manager system, and then click the OK button.

NOTE:

The Basic Configuration dialog box does not display if installation is carried out via etaconfig.ini file.
EventTracker includes several important features. You can customize EventTracker by enabling/disabling the above list of available features.

12. Click the **Finish** button to complete the installation process.
The InstallShield Wizard has successfully installed EventTrackerAgent. Click Finish to exit the wizard.
Deploy through Group Policy

Before you Begin

1. Modify `Agent.ini` and change **EM** (ENTERPRISE_MANAGER), **CM** (Change Audit manager), **INSTALLDIR** (EventTracker Agent install directory) **EP** (ENTERPRISE_PORT), **LS** (License server name/ IP Address where the digital certificate is installed), and **LP** (License server port number) value appropriately.

<table>
<thead>
<tr>
<th>Configuration Settings</th>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>[INSTALL_PATH]</td>
<td>[INSTALL_PATH]</td>
</tr>
<tr>
<td>INSTALLDIR=&lt;Installation directory if agent need to</td>
<td>INSTALLDIR=</td>
</tr>
<tr>
<td>be installed in other than default path&gt;</td>
<td>[END]</td>
</tr>
<tr>
<td>[END]</td>
<td>[ENTERPRISE_MANAGER]</td>
</tr>
<tr>
<td>EM=&lt;EventTracker Manager Hostname or IP Address&gt;</td>
<td>EM=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[ENTERPRISE_PORT]</td>
</tr>
<tr>
<td>EP=&lt;EventTracker Enterprise Port number&gt;</td>
<td>EP=14580</td>
</tr>
<tr>
<td>[END]</td>
<td>[CHANGEAUDIT_MANAGER]</td>
</tr>
<tr>
<td>CM=&lt;Change Audit Manager Hostname or IP Address&gt;</td>
<td>CM=Win2k3x64</td>
</tr>
<tr>
<td>[END]</td>
<td>[REMEDIAL_ACTIONS]</td>
</tr>
<tr>
<td>IR=1</td>
<td>IR=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[DIGITAL_CERTIFICATE]</td>
</tr>
<tr>
<td>DC= Certificate path and certificate name</td>
<td>DC=</td>
</tr>
<tr>
<td>[END]</td>
<td>[LICENSE_SERVER]</td>
</tr>
<tr>
<td>LS=&lt;The server name/ IP Address where the digital</td>
<td>LS=Win2k3x64</td>
</tr>
<tr>
<td>certificate is installed&gt;</td>
<td>[END]</td>
</tr>
<tr>
<td>[END]</td>
<td>[LICENSE_SERVER_PORT]</td>
</tr>
<tr>
<td>LP=&lt;License server port number&gt;</td>
<td>LP=14503</td>
</tr>
<tr>
<td>[END]</td>
<td>Deploy SCAP components</td>
</tr>
<tr>
<td>[DEPLOY_SCAP]</td>
<td>[DEPLOY_SCAP]</td>
</tr>
<tr>
<td>DS= ‘1’ or ‘0’</td>
<td>DS=1</td>
</tr>
<tr>
<td>[END]</td>
<td>Deploy WINSCP components</td>
</tr>
<tr>
<td>[DEPLOY_WINSCP]</td>
<td>[DEPLOY_WINSCP]</td>
</tr>
<tr>
<td>DW= ‘1’ or ‘0’</td>
<td>DW=1</td>
</tr>
<tr>
<td>[END]</td>
<td></td>
</tr>
</tbody>
</table>

Table 6
2. Create a network share on server and allow **Domain Computers** to have at least **READ** access permission.

3. Copy the **AgentMSI_7x** folder to the network share, which is created in previous step.

   Network share folder should have the below files.

   Figure 116

   ![Image of C:AgentMSI_75 folder](image)

   **Acronyms Used:**

   - **INSTALLDIR:** If this parameter is left blank, the files will be installed in the default location i.e. `%ProgramFiles%\Prism Microsystems`.
   - Else you can specify the path where you wish to install the files.
   - **EM:** If this parameter is left blank, Enterprise manager won’t be installed.
   - **EP:** If this parameter is left blank, the installer will assume the default port.
   - **CM:** If this parameter is left blank, Change Audit manager won’t be installed.
   - **IR:** If 1 then remedial actions are installed, if 0 then remedial actions are not installed. If this parameter is left blank, the installer takes a default value as “1”.
   - **DC:** The location where the certificate file is present. If left blank, the installer will assume the file to be present in the same location where the **AgentMSI** files are extracted.
   - **LS:** The system name/ IP Address where the digital certificate is installed. If this parameter is left blank, the value will be read from EM (i.e. License server name will be the same as Enterprise manager)
- **LP**: If this parameter is left blank, the default port (i.e. 14503) will be assumed by the installer.

- **DS**: Deploy SCAP components. If the value is ‘0’, then SCAP components will not be installed. If the value is ‘1’, then SCAP components will be installed.

- **DW**: Deploy WINSCP components. If the value is ‘0’, then WINSCP components will not be installed. If the value is ‘1’, then WINSCP components will be installed.

**NOTE:**
- Please rename the certificate file as “EventTracker.cer”
- All the parameters will be read from the “Agent.ini” configuration settings file, when the installer is running silently.
- It is mandatory to specify either Enterprise Manager name or Change Audit Manager name.
- If user wish to install EventTracker Agent then Enterprise Manager Name (EM) is mandatory.
- If user wish to install Change Audit Agent then Change Audit Manager Name (CM) is mandatory.
- If you wish to place the certificate file in a different location, then please provide the full path along with the certificate name in the configuration settings file (i.e. DC = full path along with the certificate name)
- Remedi**al Actions** are scripts or EXEs that can be launched at either the Agent or Manager Side, in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder.
- **Microsoft XML Core Services (MSXML)** is installed along with the MSI Agent Installer setup for 32-bit and 64-bit machines respectively.
- The **Microsoft Visual C++ 2008 Redistributable Package (x86)** which installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ is also installed along with the MSI Agent Installer setup.
- Before deploying the Agent, make sure that the Agent system(s) and domain controller are synchronized.
Launch Group Policy Management Console

1. Select the **Start** button, select **Settings**, and then select **Control Panel**.
2. Select **Administrative Tools**, and then select **Group Policy Management**.
Create the Group Policy Object in Active Directory for Software Deployment

Follow the steps given below to create the new ‘Group Policy Object’ using the ‘Group Policy Management’ Snap-in,

1. In the Group Policy Management pane, expand Domains node, and then expand domain system node.

2. Right click Group Policy Objects, and then click New.

3. Enter a name for this new GPO (Ex. AgentMSI GPO) and then click the OK button.
4. Click the name of newly created GPO. In this case, ‘AgentMSI GPO’.

A. In the **Security Filtering** pane, click the **Add** button to apply GPO settings to the domain computers group (or ensure the authenticated users group is listed).

B. In the **Enter the object name to select** field, type the object name or a part of the object name, and then click the **Check Names** button to select the object name.
C. Click the **OK** button.

5. Right click the newly created GPO, and then click **Edit**.

   **Group Policy Object Editor** window will be opened.

   A. Expand the **Computer Configuration**, and open **Software Settings**.

   ![Select User, Computer, or Group](image)

   **Figure 121**

   ![Computer Configuration](image)

   **Figure 122**

   B. Right-click **Software Installation**, select **New**, and then select **Package**.
Open window displays.

C. Locate the UNC path of the server share where the MSI installer file is located (\Server\Share\AgentMSI_7x where x is version number 1/2/3/4/5).

D. Select the MSI installer file EventTrackerAgent.msi, and then click Open.

EventTracker displays ‘Deploy Software’ dialog box. Refer Figure 125.
6. Select **Assigned**, and then click **OK**.

   You have now created and assigned the **Package Object**.

7. Right-click on the **Package Object**, and then select **Properties**.
8. Click the **Security** tab, select the **Add** button to add **Domain Computers** to provide security permissions.
   Refer Figure 126.

![Figure 125: Deploy Software](image)

![Figure 126](image)
9. Select the Advanced button, select Find Now.
   Refer Figure 127.

![Select Users, Computers, or Groups dialog box](image)

Figure 127

10. Select Domain Computers from Search results, and then select OK button.

![Select Users, Computers, or Groups dialog box](image)

Figure 128

11. Select the OK button.
12. In EventTrackerAgent Properties pane, select Read and Write permissions. Select the Advanced button. Refer Figure 128.

![Image of EventTrackerAgent Properties window](image)

**NOTE:** Ensure Domain Computers has the Read and Write rights.

13. Select Domain Computers, and then click Edit. Refer Figure 130.
14. Check the **List Contents**, **Read All Properties**, and **Read Permissions** options, if not selected. Select the **OK** button.

Refer Figure 131.

15. Select the **Apply** button and then select the **OK** button.

16. In **Group Policy Management** pane, right click the domain system name, and then select **New Organizational Unit** (OU).

A New Organizational Unit has to be created. Refer Figure 131.
17. Enter **New Organizational Unit** name.  
For example: Group Policy.

18. Right click newly created OU, and then click **Link an Existing GPO**.  
Refer Figure 132.
19. In the Select GPO dialog box, select the appropriate **domain name** and newly created **Group Policy Object**, and then click the **OK** button.

20. Close the **Group Policy window**.

The **MSI package** has now been defined and is ready for the deployment.

21. Force replication to all other domain controllers.

**NOTE:**

EventTracker and Change Audit Agents will be installed once the target machines are restarted.

If agent.ini and etaconfig.ini files are present in same folder, configuration will be deployed from etaconfig.ini file.
Verify Installation

Events will be sent to the target systems (i.e. “Manager” systems) upon successful deployment of EventTracker/ Change Audit agents. The name of the deployed agent along with their version number will appear in the System manager screen. On Target systems, following events will be generated in System Event Log:

On Win XP, Win 2003 server operating systems

On successful Agent deployment:

**Example 1:**
- Event Type : Information
- Event Source : Application Management
- Event Category: None
- Event ID : 301
- User : NT AUTHORITY\SYSTEM
- Computer : ESXWINXPVM8
- Description : The assignment of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.

**Example 2:**
- Event Type : Information
- Event Source : Application Management
- Event Category: None
- Event ID : 302
- User : NT AUTHORITY\SYSTEM
- Computer : ESXWINXPVM8
- Description : The install of application EventTrackerAgent from policy EventTracker Agent Deployment succeeded.
EventTracker Agent Deployment

Event Type : Warning
Event Source : Application Management
Event Category: None
Event ID : 102
User : NT AUTHORITY\SYSTEM
Computer : ESXWINXPVM8
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.


On Successful Agent Deployment:

Example 1:
Log Name : System
Source : Application Management Group Policy
Event ID : 301
Task Category : None
Level : Information
Keywords : Classic
User : SYSTEM
Computer : Esxwin2k8r2vm3.Toons.local
Description : The assignment of application EventTrackerAgent from policy Software Deployment policy succeeded.

Example 2:
Log Name : System
Source : Application Management Group Policy
Event ID : 302
Task Category : None
Level : Information
Keywords : Classic
User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy succeeded.

On Failed Agent Deployment:
Log Name : System
Source : Application Management Group Policy
Event ID : 102
Task Category : None
Level : Error
Keywords : Classic
User : SYSTEM
Computer : Esxwin2kBr2vm3.Toons.local
Description : The install of application EventTrackerAgent from policy Software Deployment policy failed.

Limitation for Group Policy Installation

- Retain configuration does not work via Group policy
- Upgrade agents is not supported via Group policy
- Modification features are not supported via Group policy
- Command line or silent installation doesn't support retain, upgrade and modify functions
- If EventTracker and Change Audit agent is installed via group policy then it is not possible to configure group policy to uninstall Change Audit or EventTracker agent only. While uninstalling both EventTracker and Change Audit agent will be uninstalled.
Manual Agent Install V7.5 [Batch File Install]

Installing EventTracker Agent

A. **Prepare the files for manual agent install (EventTracker Agent)**

1) Extract the zip file in the root directory of install drive.
2) Replace `Agent\AI\Temp\EvtLicenseCert.cer` with your certificate file used for ET installs. Keep the certificate name always as `EvtLicenseCert.cer`.
3) Replace `Agent\AI\Temp\etaconfig.ini` with your copy of `etaconfig.ini`.
4) Run `"%ProgramFiles%\Prism Microsystems\` on the manager system, and then copy the latest CRL file (`PrismCA.crl`).
5) Replace `Agent\AI\Temp\PrismCA.crl` with this latest CRL copied from manager system.
6) If program files shortcut menu is not required, then open the file `Agent\etsetup.ins` in notepad and replace `PgmMenuShortCutReq=1` with `PgmMenuShortCutReq=0`.

**NOTE:**

The default `etaconfig.ini` available with this installer will not have a manager and license server configured. In addition, File transfer and Config assessment are disabled. If the default copy is not replaced, then please configure Manager and required settings by opening **Programs -> EventTracker -> Agent Config** (Agent Configuration GUI) or by running `etaconfig.exe` from installation path.

B. **Perform the installation on XP/2K3 (32 bit)**

1) Execute `install.bat`.

C. **Perform the installation on XP/2K3 (64 bit)**

1) Open the file `Agent\etsetup.ins` and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".
2) Execute `installx64.bat`.

D. **Perform the installation on Vista/2k8/Win7 (32 bit) when UAC is enabled**

1) Select the **Start** button, select **All Programs**, and then select **Accessories**.
2) Right click on ‘Command Prompt’ and select ‘Run as administrator’ to open the command prompt as administrator.

3) In the command prompt, change the directory to the path where install.bat file is located.

4) Execute ‘install.bat’.

E. Perform the installation on Vista/2k8/Win7 (64 bit)

1) Select the Start button, select All Programs, and then select Accessories.

2) Right click on ‘Command Prompt’ and select ‘Run as administrator’ to open the command prompt as administrator.

3) Open the fileAgent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

4) In the command prompt, change the directory to the path where installx64.bat file is located.

5) Execute installx64.bat.

F. Perform the installation on Win 8 (32 bit OS) (supported for v7.4 and above)

1) Press the WINDOWS and X keys together and then click on Command Prompt (Admin).

2) Click Yes to the User Account Control message that appears.

3) In the command prompt, change the directory to the path where install.bat file is located.

4) Execute ‘install.bat’.

G. Perform the installation on Win 8/2012/ 2012 R2 (64 bit OS) (supported for v7.4 and above)

1) Press the WINDOWS and X keys together and then click on Command Prompt (Admin).

2) Click Yes to the User Account Control message that appears.

3) Open the fileAgent\wcsetup.ins, and update "LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows".

4) In the command prompt, change the directory to the path where installx64.bat file is located.

5) Execute installx64.bat.
EventTracker Agent Deployment

Manual Agent Installation Using ‘psexec.exe’

Execute the batch file

1. Extract attached zip file content to C:\ETAgentRemoteinstall.
   Six files will be extracted.
   a) ETManualinstall.bat
   b) ETManualinstallx64.bat
   c) EtRemotedeploy.bat
   d) EtRemotedeployx64.bat
   e) psexec.exe
   f) systems.txt

Install agents from 32 Bit Systems

1. Modify ETManualinstall.bat and update the below entry
2. xcopy "\\win2k3x64\Manualagentinstall\ET7.2b69 Agent" to Manual Agent installer folder UNC path.
3. Modify EtRemotedeploy.bat and update username (domain\username) of Authorized user on remote machines.
4. Provide the 32 bit systems list in Systems.txt
5. Launch ETRemotedeploy.bat.

Install agents from 64 Bit Systems

1. In the shared UNC path open the file Agent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent"
2. Modify ETManualinstallx64.bat and update the below entry
3. xcopy "\\win2k3x64\Manualagentinstall\ET7.2b69 Agent" to Manual Agent installer folder UNC path.
4. Modify EtRemotedeployx64.bat and update username (domain\username) of Authorized user on remote machines.
5. Provide the 64 bit systems list in Systems.txt
6. Launch EtRemotedeployx64.bat.

NOTE:
All the systems must have "C:\" drive.
To install on Vista/Win 2k8/Win 2k8 R2/Win7/Win 8/Win 2012/Win 2012 R2 systems UAC should be disabled.
For installing on Vista/Win 2k8/Win 2k8 R2/Win7/Win 8/Win 2012/Win 2012 R2 systems please change the Manual Agent Installer folder path suitably (ET7.2b69 Vista Agent) in ETManualinstall.bat & ETManualinstallx64.bat
Script can be downloaded from
www.prismmicrosys.com/Support/utils/CAAgentRemoteinstall.zip

Installing Change Audit Agent

A. **Prepare the files for manual agent install (Change Audit Agent)**

1) Extract the zip file in the root directory of install drive.
2) Replace Agent\AlTemp\EvtLicenseCert.cer with your certificate file used for ET installs. Keep the certificate name always as EvtLicenseCert.cer.
3) Replace Agent\AlTemp\ wcw.ini with your copy of wcw.ini.
4) Get latest CRL file (PrismCA.crl) by running ‘%ProgramFiles%\Prism Microsystems’ on the manager system. Replace Agent\AlTemp\PrismCA.crl with this latest CRL copied from manager system.
5) Open the file Agent\wcsetup.ins in notepad and replace ‘Server=0’ with ‘Server=<ManagerName>’. Substitute the text ‘<ManagerName>’ with the name of manager system.
6) If program files shortcut menu is not required, then open the file Agent\ wcsetup.ins in notepad, and replace ‘PgmMenuShortCutReq=1’ with ‘PgmMenuShortCutReq=0’.

B. **Perform the installation on XP/2K3 (32 bit)**

1) Execute install.bat.

C. **Perform the installation on XP/2K3 (64 bit)**

1) Open the file Agent\ etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".

2) Execute installx64.bat.

D. **Perform the installation on Vista/2k8/Win7 (32 bit) when UAC is enabled**
EventTracker Agent Deployment

1) Select the **Start** button, select **All Programs**, and then select **Accessories**.

2) Right click on ‘**Command Prompt**’ and select ‘**Run as administrator**’ to open the command prompt as administrator.

3) In the command prompt, change the directory to the path where **install.bat** file is located.

4) Execute ‘**install.bat**’.

E. **Perform the installation on Vista/2k8/Win 7 (64 bit)**

1) Select the **Start** button, select **All Programs**, and then select **Accessories**.

2) Right click on ‘**Command Prompt**’ and select ‘**Run as administrator**’ to open the command prompt as administrator.

3) In the command prompt, change the directory to the path where **install.bat** file is located.

4) Open the file **Agent\wcsetup.ins**, and update "**LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows**".

5) Execute **installx64.bat**.

F. **Perform the installation on Win 8 (32 bit OS) (supported for v7.4 and above)**

1) Press the **WINDOWS** and **X** keys together and then click on **Command Prompt (Admin)**.

2) Click **Yes** to the User Account Control message that appears.

3) In the command prompt, change the directory to the path where **install.bat** file is located.

4) Execute ‘**install.bat**’ and press enter.

G. **Perform the installation on Win 8/2012/ 2012 R2 (64 bit OS) (supported for v7.4 and above)**

1) Press the **WINDOWS** and **X** keys together and then click on **Command Prompt (Admin)**.

2) Click **Yes** to the User Account Control message that appears.

3) Open the file **Agent\wcsetup.ins**, and update "**LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows**".

4) In the command prompt, change the directory to the path where **installx64.bat** file is located.

5) Execute **installx64.bat**.

**NOTE:**
If you are installing EventTracker agent or change audit agent in custom path using batch file installer, then you need to change the custom installation path in *.ins and *.bat file as well.

Change Audit Agent Installation Using ‘psexec.exe’

Execute the batch file

1. Extract attached zip file content to C:\CAAgentRemoteinstall.
   Six files will be extracted.
   a) CAManualinstall.bat
   b) CAManualinstallx64.bat
   c) CARemotedeploy.bat
   d) CARemotedeployx64.bat
   e) psexec.exe
   f) systems.txt

Install agents from 32 Bit Systems

1. Modify CAManualinstall.bat and update the below entry
   xcopy "\win2k3x64\Manualagentinstall\ET7.2b69 ChangeAudit Agent" to Manual Agent installer folder UNC path.
2. Modify CARemotedeploy.bat and update username (domain\username) of Authorized user on remote machines.
3. Provide the 32 bit systems list in Systems.txt
4. Launch CARemotedeploy.bat.

Install agents from 64 Bit Systems

1. In the shared UNC path open the file Agent\wcsetup.ins and update "LocalRootDir=\Program Files (x86)\Prism Microsystems\WCWindows".
2. Modify CAManualinstallx64.bat and update the below entry
   xcopy "\win2k3x64\Manualagentinstall\ET7.2b69 ChangeAudit Agent" to Manual Agent installer folder UNC path.
3. Modify CARemotedeployx64.bat and update username (domain\username) of Authorized user on remote machines.
4. Provide the 64 bit systems list in Systems.txt
5. Launch CARemotedeployx64.bat.

NOTE:

All the systems must have "C:" drive.
To install on Vista/Win 2k8/Win 2k8 R2/Win 7/Win 8/Win 2012/ Win 2012 R2 systems UAC should be disabled. Script can be downloaded from www.prismmicrosys.com/Support/utils/CAAgentRemoteinstall.zip

Uninstall EventTracker Agent

There are various methods to uninstall EventTracker Agent

- Uninstall via Add or Remove Programs
- Uninstall via Group Policy

Uninstall via Add or Remove Programs

1. Select the Start button, select All Programs, and then select Control Panel.
2. Select Add or Remove Programs, select EventTracker Agent, and then select Remove.

A message displays. Refer Figure 133.

![Windows Installer](image)

Figure 133
3. Select the **Yes** button.

A message displays. Refer Figure 134.

4. Select **Yes/No** button.
Uninstall via Group Policy

1) In Group Policy Management window, select Group Policy Objects, select the group policy object created (i.e. in this example, AgentMSI GPO is the group policy object created), and then select Edit.

![Figure 135 Group Policy Object Editor](image)

Group Policy Object Editor window displays.

2) Select Computer Configuration, select Software Settings, and then select Software installation.

3) Right-click EventTrackerAgent, select All Tasks, and then select Remove. Refer Figure 136.
Remove Software window displays **Select removal method** option.

![Remove Software window](image)

**Figure 137**

4) Select the required option and then select the **OK** button.

**NOTE:**

If installation is carried out via Group Policy, then it should be uninstalled via Group Policy.