How to - Install EventTracker Windows and Change Audit Sensor

EventTracker Sensor Deployment User Manual

Publication Date: February 25, 2020
Abstract

EventTracker Sensor deployment processes are described in detail in this manual for v 9.2 and above. EventTracker Sensor can be deployed using methods like Active Directory Group Policy, Command Line and User Interface. The purpose of this document is to provide the step by step instructions to deploy EventTracker Sensor using various methods and understand the deployment procedure.

Audience

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

Note: The figures appearing in the document may vary according to the version to be installed.

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

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

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

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

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

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

1. Benefits/Advantages of EventTracker Sensor ................................................................. 3
2. Before You Begin .................................................................................................................. 3
3. Operating system supported: ............................................................................................. 5
5. EventTracker v9.2 and above ............................................................................................ 6
6. Deploying through Command Prompt ............................................................................... 6
   6.1 Parameters used for GUI and Silent Installation ............................................................ 6
   6.2 GUI MSI Installation: .................................................................................................... 9
      6.2.1 Procedure to install with etaconfig.ini files ............................................................ 18
   6.3 Silent EventTracker Sensor Installation ....................................................................... 23
   6.4 Uninstalling EventTracker Sensor .............................................................................. 25
7. Deploying through Agent.ini file .................................................................................... 26
   7.1 GUI MSI Installation ..................................................................................................... 26
   7.2 Silent Installation ......................................................................................................... 30
8. Deploying through Group Policy ...................................................................................... 33
   8.1 Before you Begin .......................................................................................................... 33
   8.2 Creating a network share .............................................................................................. 34
   8.3 Assigning Systems to New Organization Unit .............................................................. 42
   8.4 Launching Group Policy Management Console .......................................................... 43
   8.5 Creating the Group Policy Object in Active Directory for Software Deployment ........... 44
   8.6 Verify Installation ........................................................................................................ 54
   8.7 Uninstalling EventTracker Sensor via GPO ................................................................. 55
   8.8 Limitation for Group Policy Installation ....................................................................... 56
1. Benefits/Advantages of EventTracker Sensor

- 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
- Monitor file and registry changes on the system
- Monitor the suspicious activity.

2. Before You Begin

Before you begin with EventTracker sensor 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 sensor 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 Sensor, .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.
• **For Windows 8/8.1/2012/2012 R2/10/2016,2019** 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.

• 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 9.2** and above, 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 v9.2 and above, while configuring VMware, it throws an error message, which is displayed below:

![EventTracker Agent Configuration](image)

*Figure 1*

• Then, the user will have to register **EtVMagent.dll**.

• To register, please follow the below steps:
  ➢ Change the directory to the location where Sensor 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 Sensor, 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.

3. Operating system supported:

<table>
<thead>
<tr>
<th>Windows Platforms</th>
<th>32 bit</th>
<th>64 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2019</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2012 R2</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2012</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2008 R2</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2008</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 8, 8.1</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 10</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

EventTracker Agent for Solaris: Solaris 9, Solaris 10
4. **Download and Preparing EventTracker Sensor 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,

5. **EventTracker v9.2 and above**

1. Download MSI package (V9.2 is considered in this example AgentMSI_92.zip) from the location provided by EventTracker Support team.

2. Extract AgentMSI_92.zip to AgentMSI_92\.

![Figure 3](image)

6. **Deploying through Command Prompt**


6.1 **Parameters used for GUI and Silent Installation**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Selection of EventTracker Sensor feature from the Command line.</td>
</tr>
<tr>
<td></td>
<td>1 – Installation of EventTracker Sensor feature is selected.</td>
</tr>
<tr>
<td></td>
<td>0 – EventTracker Sensor Feature is not selected for installation.</td>
</tr>
<tr>
<td>CA</td>
<td>Selection of Change Audit feature from the Command line.</td>
</tr>
<tr>
<td></td>
<td>1 – Installation of Change Audit feature is selected.</td>
</tr>
<tr>
<td></td>
<td>0 – Change Audit Feature is not selected for installation.</td>
</tr>
<tr>
<td>CUSTOMCONFIG</td>
<td>0 – Enterprise configuration file in UDP mode</td>
</tr>
<tr>
<td></td>
<td>2 – Customer Existing etaconfig.ini.</td>
</tr>
<tr>
<td></td>
<td>3 - Enterprise Configuration file in TCP mode.</td>
</tr>
</tbody>
</table>
### EventTracker Sensor Deployment User Manual

#### Table 1

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR (For GUI)</td>
<td>Custom Installation directory path</td>
</tr>
<tr>
<td>INSTALLPATH (For Silent)</td>
<td>Custom Installation directory path</td>
</tr>
<tr>
<td>EM</td>
<td>Enterprise Manager name</td>
</tr>
<tr>
<td>EP</td>
<td>Enterprise port</td>
</tr>
<tr>
<td>CM</td>
<td>Change Audit Manager name</td>
</tr>
<tr>
<td>IR</td>
<td>Remedial Actions 1 - Predefined scripts will be placed in the EventTracker\Agent\Script folder.</td>
</tr>
<tr>
<td>LS</td>
<td>License Server</td>
</tr>
<tr>
<td>LP</td>
<td>License Port</td>
</tr>
<tr>
<td>DW</td>
<td>Deploy WinSCAP feature 1 – It will get installed 0 – It will not get installed</td>
</tr>
<tr>
<td>SC</td>
<td>shortcut 1 - shortcut enable 0 - means disable</td>
</tr>
<tr>
<td>MIN_GUI</td>
<td>Minimal GUI 1 - Minimal GUI enable 0 - Full GUI wizard.</td>
</tr>
<tr>
<td>IS_SUFFIX</td>
<td>Enable Suffix 2- enable (Location Name window will not appear) (any configuration) 1 - enable (GUI will contain control to take input as suffix) 0 - disable (no extra GUI control)</td>
</tr>
<tr>
<td>SUFFIX</td>
<td>Suffix string</td>
</tr>
<tr>
<td>SUPPORT_CONTACTS</td>
<td>Support Details</td>
</tr>
</tbody>
</table>
| PIP                             | Protection IP  
If the user provides PIP, the IP address needs to be added here. When IP address is provided, the “protect_flag” is enabled and provided IP will appear in “protect_ip” field. |
| Agent.ini                       | Agent.ini 0=Command prompt installation (It won’t consider agent.ini details) 1= Considers Agent.ini filled details |

**NOTE:** By default, EventTracker Sensor and Change Audit Sensor features are installed.
**Mandatory Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EM</td>
<td>Mandatory Parameter</td>
</tr>
</tbody>
</table>

Default values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>1</td>
</tr>
<tr>
<td>CA</td>
<td>1</td>
</tr>
<tr>
<td>CUSTOMCONFIG</td>
<td>0</td>
</tr>
<tr>
<td><strong>INSTALLDIR</strong> (For GUI mode)</td>
<td>Custom installation path</td>
</tr>
<tr>
<td><strong>INSTALLPATH</strong> (For Silent mode)</td>
<td>Custom installation path</td>
</tr>
<tr>
<td>EP</td>
<td>14505</td>
</tr>
<tr>
<td>CM</td>
<td>default value EM name</td>
</tr>
<tr>
<td>IR</td>
<td>1 (Remedial Action scripts are deployed in the Agent directory) For etaconfig.ini (Remedial action is disabled)</td>
</tr>
<tr>
<td>LS</td>
<td>default value EM name</td>
</tr>
<tr>
<td>LP</td>
<td>14503</td>
</tr>
<tr>
<td>SC</td>
<td>0</td>
</tr>
<tr>
<td>IS_SUFFIX</td>
<td>0</td>
</tr>
<tr>
<td>SUFFIX</td>
<td>exists if IS_SUFFIX=1, please provide the suffix name</td>
</tr>
<tr>
<td>DW</td>
<td>0</td>
</tr>
<tr>
<td>MIN_GUI</td>
<td>0</td>
</tr>
<tr>
<td>AGENTINI</td>
<td>0</td>
</tr>
</tbody>
</table>

**Table 2**

**If the user wants MAC address as Suffix, then the SUFFIX =“<%MAC%>”.

**If there is space in the attribute values in command line, then the user has to pass those values in double quotes (“”)**
6.2 GUI MSI Installation:

1. Extract the MSI Package. It will contain the below files:

![Figure 4](image1.png)

2. Edit the **Agent.ini** file and change the value of Agent.ini=0.

![Figure 5](image2.png)

**NOTE:**

***Please refer the above-mentioned parameter abbreviation (i.e. Table 1 and 2).***

- If the EA and CA field are not provided, by default it will install the EventTracker Sensor and the Change Audit Sensor.
- If the user wants to install only the EventTracker Sensor, then the CA should be equal to 0 and vice-versa.

3. After making the changes, save the Agent.ini file.
4. Now launch the Command prompt and “Run as Administrator”.
5. Change directory to AgentMSI_92.

Types of installation providing command in Command prompt:

1. EventTrackerSensor.msi CUSTOMCONFIG=0 EM = (Manager name) - Enterprise etaconfig.ini in UDP mode
2. EventTrackerSensor.msi CUSTOMCONFIG=3 EM = (Manager name) - Enterprise etaconfig.ini in TCP mode
3. EventTrackerSensor.msi CUSTOMCONFIG=2 - Customer Existing etaconfig.ini.

Example 1:
EventTrackerSensor.msi EA=1 CA=1 CUSTOMCONFIG=0 or 3 EM=Enterprise Manager name EP=Manager port number CM=Change Audit Manager name IR=1 LS=License server name LP=License port number MIN_GUI=0 IS_SUFFIX=1 SUFFIX=Suffix name SUPPORT_CONTACTS=Contact details.

![Image](image.png)

Figure 6

InstallShield Wizard pop up window appears on the screen.

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

4. In **Custom Setup**, select **EventTracker Sensor** and **Change Audit Sensor** based on the requirement.

![Custom Setup](image)

**Figure 8**

Click the **Next >** button.

**Figure 9**

Click ![icon](image) icon to select the installation options:

- ![This feature will be installed on local hard drive](image)
- ![This feature, and all subfeatures, will be installed on local hard drive](image)
- ![This feature will not be available](image)

**Figure 10**

- 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.
5. Click the **Change** button to change the installation path of the agent and then click the **Next >** button.

![Image](image1.png)

**Figure 11**

6. In the configuration screen, it will fetch the details from the command line. Click **Next**.

![Image](image2.png)
7. The location name will be fetched from the command line. Click **Install**.

![Figure 13](image)

**NOTE:** Allowed special characters: “-“,”_”,”.” and the characters are limited to 100.

8. Click the **Finish** button to complete the installation process.

![Figure 14](image)
9. Once it is installed successfully, it will launch the server connectivity status window which displays the connectivity status.

![Server Connectivity Status](image)

**Example 2:** EventTrackerSensor.msi CUSTOMCONFIG=0 or 3 EM=Enterprise Manager name MIN_GUI=1

![Command Prompt](image)

1. Click the **Next >** button to start with installation.
2. Ready to install wizard will be displayed. Click on **Install**.

![Ready to install wizard](image)
3. Once the installation completes, the below screen gets displayed. Click **Finish**.

![EventTracker Sensor 9.2 Installation](image)

**Figure 19**

4. Once it is installed successfully, it will launch the server connectivity status window which displays the connectivity status.

![Server Connectivity Status](image)

**Figure 20**
6.2.1 Procedure to install with etaconfig.ini files

1. Extract the MSI Package. It will contain the below files:

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent.ini</td>
<td>12/30/2019 3:13 PM</td>
<td>Configuration settings</td>
<td>3 KB</td>
</tr>
<tr>
<td>etaconfig.ini</td>
<td>12/30/2019 3:01 AM</td>
<td>Configuration settings</td>
<td>75 KB</td>
</tr>
<tr>
<td>EventTrackerSensor.msi</td>
<td>12/24/2019 3:41 PM</td>
<td>Windows Installer</td>
<td>40,835 KB</td>
</tr>
<tr>
<td>ReadMe.txt</td>
<td>12/18/2019 6:33 PM</td>
<td>Text Document</td>
<td>5 KB</td>
</tr>
</tbody>
</table>

**Figure 21**

2. Edit the **Agent.ini** file and change the value of Agent.ini=0.

![Agent.ini file content](image)

**Figure 22**

**NOTE:**

- For this type of installation the user should keep the customized etaconfig.ini file in the extracted MSI package path.

- The attributes needs to filled in the etaconfig.ini for **CUSTOMCONFIG=2**. When the user is using the customized etaconfig.ini file, they should not run any parameters in the command line except “EventTrackerSensor.msi CUSTOMCONFIG=2”.
To install the sensor with customized etaconfig.ini file,

- Launch Command prompt and “Run as Administrator”.
- Change directory to AgentMSI_92.
- Enter the below command:

`EventTrackerSensor.msi CUSTOMCONFIG=2`

![Command prompt screenshot](image)

**Figure 23**

1. It will launch the welcome screen. Click **Next**.

![Welcome screen](image)

**Figure 24**

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

4. In **Custom Setup**, select **EventTracker Sensor** and **Change Audit Sensor** based on the requirement.
• Click icon to select the installation options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📁 This feature will be installed on local hard drive.</td>
<td></td>
</tr>
<tr>
<td>🚦 This feature, and all subfeatures, will be installed on local hard drive.</td>
<td></td>
</tr>
<tr>
<td>✗ This feature will not be available.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 27

• 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.

5. Click the Change button to change the installation path of the agent and then click the Next > button.

6. Click Next.
7. In this last step of the installation process, click the **Install** button.
8. Click the **Finish** button to complete the installation process.

![EventTracker Sensor 9.2](image)

**Figure 31**

### 6.3 Silent EventTracker Sensor Installation

1. Go to Command prompt, right click and “Run as Administrator”.
2. Change directory to **AgentMSI_92**.
3. Types the below commands based on the requirement

<table>
<thead>
<tr>
<th>Mandatory Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>EM</td>
</tr>
</tbody>
</table>
Default values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>1</td>
</tr>
<tr>
<td>CA</td>
<td>1</td>
</tr>
<tr>
<td>CUSTOMCONFIG</td>
<td>0</td>
</tr>
<tr>
<td>INSTALLPATH</td>
<td>Custom installation path</td>
</tr>
<tr>
<td>EP</td>
<td>14505</td>
</tr>
<tr>
<td>CM</td>
<td>default value EM name</td>
</tr>
<tr>
<td>IR</td>
<td>1 (Remedial Action scripts are deployed in the Agent directory) For etaconfig.ini (Remedial action is disabled)</td>
</tr>
<tr>
<td>LS</td>
<td>default value EM name</td>
</tr>
<tr>
<td>LP</td>
<td>14503</td>
</tr>
<tr>
<td>IS_SUFFIX</td>
<td>0</td>
</tr>
<tr>
<td>SUFFIX</td>
<td>exists if IS_SUFFIX=1, please provide the suffix name</td>
</tr>
</tbody>
</table>

**Example 1:**

EventTrackerSensor.msi /qn CUSTOMCONFIG=0 or 3 EM=(Manager name)

![Command Prompt](image)

**Example 2:** EventTrackerSensor.msi EA=1 CA=1 CUSTOMCONFIG=0 or 3 EM=Enterprise Manager name EP=Manager port number CM=Change Audit Manager name IR=1 LS=License server name LP=License port number DW=Deploy WinScap IS_SUFFIX=1 SUFFIX=Suffix name SUPPORT_CONTACTS=Contact details.
Example 3: EventTrackerSensor.msi /qn CUSTOMCONFIG=2 - Customer Existing etaconfig.ini.

NOTE:

- For this type of installation the user should keep the customized etaconfig.ini file in the extracted MSI package path.
- The attributes needs to filled in the etaconfig.ini for CUSTOMCONFIG=2. When the user is using the customized etaconfig.ini file, they should not run any parameters in the command line except “EventTrackerSensor.msi /qn CUSTOMCONFIG=2”.

6.4 Uninstalling EventTracker Sensor

- Go to the Control Panel and Program & Features.
- Select the EventTracker sensor and Uninstall it.

After the un-installation is complete, you can verify whether the agent files in registry, the install path and the services were removed or not.
It will write the Event ID 3209, in the manager.

**Sample description:**

event_description: Detected software EventTracker Sensor has been uninstalled from this system.

Name: EventTracker Sensor

Agent Type: EventTracker Agent and Change Audit

Agent Version: 9.2

User Name: NTPL\Karen

### 7. Deploying through Agent.ini file

#### 7.1 GUI MSI Installation

1. Extract the MSI Package. It will contain the below files:

   ![Figure 36](image)

   **Figure 36**

2. Edit the `Agent.ini` file and change the value of Agent.ini=1.

**NOTE:** Mandatory Fields to fill in the `Agent.ini` file are EM, EP, CM (if the user is installing Change Audit), LS, LP, CUSTOMCONFIG, CA, EA and AGENTINI.
NOTE:

***Please refer the above-mentioned parameter abbreviation (i.e. Table 1 and 2).

- If the user wants to install only the EventTracker Sensor, then the CA should be equal to 0 and vice-versa.

Types of installation using Agent.ini for GUI Mode:

1. CUSTOMCONFIG=0 EM = (Manager name) - Enterprise etaconfig.ini in UDP mode.

   ✓ Here, fill the Agent.ini file with the mandatory fields that were shown in Figure: 37 and change the CUSTOMCONFIG=0
An example of an Agent.ini with the changed field is shown below.

```
[CONFIGURATION]
CUSTOMCONFIG=3
[END]
```

Figure 38

✓ Fill the other required parameters in the Agent.ini file, as per requirement.
✓ Now save the Agent.ini file and then open the Command Prompt as “Run as Administrator”.
✓ Change directory to **AgentMSI_92**.
✓ Type the below command and hit Enter.

```
EventTrackerSensor.msi
```

Figure 39

✓ It will display the Installation screens (Refer **Figure 7 to Figure 15**)

ii. **CUSTOMCONFIG=3 EM = (Manager name)** - Enterprise etaconfig.ini in TCP mode

✓ Here, fill the Agent.ini file with the mandatory fields that were shown in **Figure: 37** and change the **CUSTOMCONFIG=3**

```
[CONFIGURATION]
CUSTOMCONFIG=3
[END]
```

Figure 40

✓ Fill the other required parameters in the Agent.ini file, as per requirement.
✓ Now save the Agent.ini file and then open the Command Prompt as “Run as Administrator”.
✓ Change directory to **AgentMSI_92**.
✓ Type the below command and hit Enter.

```
EventTrackerSensor.msi
```

EventTrackerSensor.msi
iii. CUSTOMCONFIG=2 - Customer Existing etacfg.ini.

NOTE: Please make sure the custom etacfg.ini is kept in the extracted MSI package as shown below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>1/2/2019 5:46 AM</td>
<td>Configuration sett...</td>
<td>3 KB</td>
</tr>
<tr>
<td>etaconfig</td>
<td>1/24/2019 3:10 PM</td>
<td>Configuration sett...</td>
<td>76 KB</td>
</tr>
<tr>
<td>EventTrackerSensor</td>
<td>1/23/2019 11:27 AM</td>
<td>Windows Installer...</td>
<td>40,025 KB</td>
</tr>
<tr>
<td>ReadMe</td>
<td>9/11/2018 12:50 AM</td>
<td>Text Document</td>
<td>4 KB</td>
</tr>
</tbody>
</table>

✓ Here, fill the Agent.ini file only with the mandatory fields i.e. (EA=1, CA=1, Agent.ini=1) and change the CUSTOMCONFIG=2

:Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=2
[END]

✓ Now save the Agent.ini file and then open the Command Prompt as “Run as Administrator”.
✓ Change directory to AgentMSI_92.
✓ Type the below command and hit Enter.

EventTrackerSensor.msi

✓ It will display the Installation screens (Refer Figure 7 to Figure 15)
7.2 Silent Installation

1. Extract the MSI Package. It will contain the below files:

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>1/2/2019 5:46 AM</td>
<td>Configuration sett...</td>
<td>3 KB</td>
</tr>
<tr>
<td>EventTrackerSensor</td>
<td>1/23/2019 11:27 AM</td>
<td>Windows Installer ...</td>
<td>40,025 KB</td>
</tr>
<tr>
<td>ReadMe</td>
<td>9/11/2018 12:50 AM</td>
<td>Text Document</td>
<td>4 KB</td>
</tr>
</tbody>
</table>

Figure 45

2. Edit the Agent.ini file and change the value of Agent.ini=1.

3. Mandatory Fields to fill in the Agent.ini file are EM, EP, CM (if the user is installing Change Audit), LS, LP, CUSTOMCONFIG, CA, EA and AGENTINI. (Refer Figure: 37).

NOTE:

***Please refer the above-mentioned parameter abbreviation (i.e. Table 1 and 2).

- If the user wants to install only the EventTracker Sensor, then the CA should be equal to 0 and vice-versa.

Types of installation using Agent.ini for Silent Mode:

i. CUSTOMCONFIG=0 EM = (Manager name) - Enterprise etaconfig.ini in UDP mode.

✓ Here, fill the Agent.ini file with the mandatory fields that were shown in Figure: 37 and change the CUSTOMCONFIG=0

An example of an Agent.ini with the changed field is shown below.

```
Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=0
[END]
```

Figure 46

✓ Fill the other required parameters in the Agent.ini file, as per requirement.
✓ Now save the Agent.ini file and then open the Command Prompt as “Run as Administrator”.
✓ Change directory to AgentMSI_92.
✓ Type the below command and hit Enter.

```
EventTrackerSensor.msi /qn
```
✓ The sensor will take some time to get installed. For verifying, you can go to the Install Directory and check the folder structure.

ii. CUSTOMCONFIG=3 EM = (Manager name) - Enterprise etaconfig.ini in TCP mode.

✓ Here, fill the Agent.ini file with the mandatory fields that were shown in Figure: 3 and change the CUSTOMCONFIG=3

An example of an Agent.ini with the changed field is shown below.

```ini
;Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=3
[END]
```

✓ Fill the other required parameters in the Agent.ini file, as per requirement.
✓ Now save the Agent.ini file and then open the Command Prompt as “Run as Administrator”.
✓ Change directory to AgentMSI_92.
✓ Type the below command and hit Enter.

EventTrackerSensor.msi /qn

✓ The sensor will take some time to get installed. For verifying, you can go to the Install Directory and check the folder structure.

iii. CUSTOMCONFIG=2 - Customer Existing etaconfig.ini.

NOTE: Please make sure the custom etaconfig.ini is kept in the extracted MSI package as shown below:
✓ Here, fill the Agent.ini file only with the mandatory fields i.e. (EA=1, CA=1, Agent.ini=1) and change the CUSTOMCONFIG=2

```plaintext
;Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=2
[END]
```

Figure 51

✓ Now save the Agent.ini file and then open the Command Prompt as “Run as Administrator”.

✓ Change directory to AgentMSI_92.

✓ Type the below command and hit Enter.

`EventTrackerSensor.msi /qn`

Figure 52

✓ The sensor will take some time to get installed. For verifying, you can go to the Install Directory and check the folder structure.
8. Deploying through Group Policy

8.1 Before you Begin

1. Modify Agent.ini and change EM (ENTERPRISE_MANAGER), CM (Change Audit manager), INSTALLDIR (EventTracker sensor install directory for custom path), EP (ENTERPRISE_PORT), LS (License server name/IP Address where the digital certificate is installed), LP (License server port number), CUSTOMCONFIG (Generic=0, Custom=2 & Generic with TCP=3), CA (CHANGEAUDITFEATURE), EA (EVENTTRACKERAGENTFEATURE), Agentini (AGENTINI) value appropriately. The other fields can also be changed as per requirement.

<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=14505</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 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>
<tr>
<td>Setup wizard with minimal GUI</td>
<td>Setup wizard with minimal GUI</td>
</tr>
<tr>
<td>[MINIMAL_GUI]</td>
<td>[MINIMAL_GUI]</td>
</tr>
<tr>
<td>MIN_GUI=’1’ or ’0’</td>
<td>MIN_GUI=1</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>Ask for suffix is enable or not</td>
<td>Ask for suffix is enable or not</td>
</tr>
<tr>
<td>[ENABLE_SUFFIX]</td>
<td>[ENABLE_SUFFIX]</td>
</tr>
<tr>
<td>IS_SUFFIX=0</td>
<td>IS_SUFFIX=1</td>
</tr>
<tr>
<td>[END]</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.

8.2 Creating a network share

1. Go to **Server Manager** and click on **File and Storage Services**.
2. Click on **Shares** in the left pane.

3. Now, right click on the screen and select **New Share**.
4. Select File share profile and click **Next**.

5. Click on **Next**.
6. Now type the Folder Name to be shared and then click **Next**.
7. Click **Next** to proceed.

![Image of New Share Wizard](image1)

Figure 59

8. The below shown access should be allowed for successful installation. Click **Next**.

![Image of Permissions](image2)

Figure 60
9. Confirm the details and click **Create**.

![Figure 61](image1)

10. Once the creation is completed click on **Close**.

![Figure 62](image2)
3. Copy the **AgentMSI_92** folder to the network share, which is created.

Network share folder should have the below files.

![Figure 63](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>1/2/2019 5:46 AM</td>
<td>Configuration sett...</td>
<td>3 KB</td>
</tr>
<tr>
<td>EventTrackerSensor</td>
<td>1/23/2019 11:27 AM</td>
<td>Windows Installer ...</td>
<td>40,025 KB</td>
</tr>
<tr>
<td>ReadMe</td>
<td>9/11/2018 12:50 AM</td>
<td>Text Document</td>
<td>4 KB</td>
</tr>
</tbody>
</table>

**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**: Specify the EventTracker manager name. Agent will send events to the manager specified here.

- **EP**: Specify the port number on which you wish to send events to EventTracker manager.

- **CM**: Specify the Change Audit manager name.

- **IR**: If 1 then remedial actions are installed, if 0 then remedial actions are not installed.

- **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.

- **DW**: Deploy WINSCP components. If the value is empty then WINSCP components will not be installed. If the value is ‘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.

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

• **SUFX:** Enter the system suffix name in this field.

• **MESSAGE:** Customized Contact details

• **CUSTOMCONFIG:** Usage of custom config ini file

  ✓ EventTrackerSensor.msi CUSTOMCONFIG=0 EM = (Manager name) - Enterprise etaconfig.ini in UDP mode.
  ✓ EventTrackerSensor.msi CUSTOMCONFIG=3 EM = (Manager name) - Enterprise etaconfig.ini in TCP mode.
  ✓ EventTrackerSensor.msi CUSTOMCONFIG=2 - Customer Existing etaconfig.ini.

• **PIP:** Usage of Protect IP

• **CA:** To install Change Audit

• **EA:** To install EventTracker agent

• **AGENTINI:** To use agent.ini or command parameters (Usage of agent.ini=1, Usage of command parameters=0)

**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.

• 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.

• The checkbox setting in GUI i.e “Deploy WINSCP 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.

### 8.3 Assigning Systems to New Organization Unit

In the Active Directory domain machine, click **Windows + R** and type “**dsa.msc**”.

1. Right click the group, select new and then Organizational Unit.

   ![Figure 64](image)

2. Enter a Name and click **OK**.
3. Now move the systems to the newly created OU Group.

![New Object - Organizational Unit](image)

Figure 65

![Group Policy Management](image)

Figure 66

### 8.4 Launching 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**.
8.5 Creating 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**.

![Software Settings Tree](image)

Figure 72

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

![Software Installation Pane](image)

Figure 73

**Open** window displays.
A. Locate the UNC path of the server share where the MSI installer file is located (\XXXX\AgentMSI_92).  
B. Select the MSI installer file EventTrackerAgent.msi, and then click Open.  

EventTracker displays ‘Deploy Software’ dialog box.

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.
1. Enter “Domain Computers” and click OK.

2. Now select the **Advanced** button, click **Add** and then Select Principal.
3. Enter “Domain Computer” and click OK.

4. Check the List Contents, Read All Properties, and Read Permissions options, if not selected. Select the OK button.
NOTE:

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

5. Select the **Apply** button and then select the **OK** button.
6. In the EventTracker Sensor Properties window, click **OK**.
7. In **Group Policy Management** pane, right click new organizational unit created earlier (Refer Figure: 65 and 66) and select Link Existing GPO option.
8. Now select the created GPO and click OK.

9. Navigate to Linked GPO, right-click and enable the Enforced.
The **MSI package** has now been defined and is ready for the deployment.

Now the user can go to Target machine and update the Group policy by using the command in command prompt.

```bash
gpupdate /force
```

![Figure 83](image)

**Figure 83**

**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 the same folder, and the CUSTOMCONFIG=2 in the Agent.ini file, then configuration will be deployed from etaconfig.ini file.

1. Once the gpo is updated, you can verify the folder structure in the target machine as shown below:
8.6 Verify Installation

Events will be sent to the target systems (i.e. "Manager" systems) upon successful deployment of EventTracker/ Change Audit Sensors. 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 Successful Agent Deployment:

Sample Event ID and Description

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>MsiInstaller</td>
</tr>
<tr>
<td>Event ID</td>
<td>1040</td>
</tr>
<tr>
<td>Task Category</td>
<td>None</td>
</tr>
<tr>
<td>Level</td>
<td>Information</td>
</tr>
<tr>
<td>Keywords</td>
<td>Classic</td>
</tr>
<tr>
<td>User</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>Computer</td>
<td>Test-10-HC.pcloud2008.com</td>
</tr>
</tbody>
</table>
8.7 Uninstalling EventTracker Sensor via GPO

1. Edit the linked Group Policy Object i.e (AgentMSI_92) and navigate to Policies>Software Settings>Software Installation and select the msi.
2. Now right click and select All Task and then Remove.

![Group Policy Management Editor](image)

Figure 86

Now the user can go to Target machine and update the Group policy by using the command in command prompt.

```
gpupdate /force
```

![Command Prompt](image)

Figure 87

It gets successfully uninstalled.
8.8 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.