

# EventTracker Manual Agent Deployment

User Manual

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

Publication Date: August 14, 2012

## Abstract

EventTracker agent deployment processes are described in detail in this manual. EventTracker Agent can be deployed using methods like Active Directory Group Policy, Command Line, User Interface, and using any other Software deployment software. This document has covered all the methods to deploy an agent.

## Purpose

The purpose of this document is to provide the step by step instructions to deploy EventTracker Agent using various methods, and to enable the user to understand the deployment procedure.

## Target audience

EventTracker users or system administrators, who wish to deploy the EventTracker agent.

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

This document is for informational purposes only. Prism Microsystems, Inc. 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 Guide may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, Inc. 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.

© 2012 Prism Microsystems, Inc. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



## **Table of Contents**

Before You Begin	3
Download and Prepare EventTracker Agent MSI Installer Package for Deployment	4
Deployment through Command Line	4
Deployment through User Interface	6
Deployment through Group Policy	12
Before you Begin	12
Launch Group Policy Management Console	15
Create the Group Policy Object in Active Directory for Software Deployment	15
Verifying Installation	24
On Pre-Vista Operating System:	24
On Vista and Post-Vista Operating System:	26
Limitation for Group Policy Installation	28
Manual Agent Installation [Batch File Install]	28
EventTracker Agent Installation	28
Change Audit Agent Installation	29



## 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,

- 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 systems 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.

## \rm CAUTION:

- To complete the installation, target systems 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 computers boot or login will be
  delayed until the second boot or login.



# 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,

- 1. Download MSI package (e.g. AgentMSI\_73.zip) from the location provided by Prism Microsystems Support team.
- 2. Extract AgentMSI\_73.zip to AgentMSI\_73\.
- 3. Copy License certificate file to Extracted folder (AgentMSI\_73) and rename it to EventTracker.cer.

## Deployment through Command Line

- 1. Fill the necessary details in 'Agent.ini" configuration file (refer Table 1 on how to specify the parameters).
- 2. The installer will look for the certificate file to be present in the same folder (See the highlighted file in the figure 1) where the files are extracted. So, please copy the certificate file to **AgentMSI\_73** folder.

Address 🚞 \\popeye\Shared\AgentMSI_73		
Name 🔺	Size	
💁 Agent.ini	2 KB	
Change~1.cab	3,755 KB	
etwAgent73.exe	4,585 KB	
EventT~1.cab	10,939 KB	
EventTracker.cer	3 KB	
🔁 Event Tracker Agent. msi	19,812 KB	
🗐 ReadMe.txt	2 KB	
ڬ setup.bmp	589 KB	
El anno 1		

Figure 1

- 3. To launch command line, click the **Start** button, and then click **Run**.
- 4. In **Run** dialog box, type '**CMD'**, and then click the '**Ok'** button.
- 5. Change directory to AgentMSI\_73
- 6. Type **'EventTrackerAgent.msi /qn'** command, and then click the **Enter** button.



## NOTE:

- On Post-Vista machines, 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 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).



## Deployment through User Interface

1. Click on etwAgent73.exe.

InstallShield Wizard pop up window appears on the screen.



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'.

👹 EventTrackerAgent 7.3	×
License Agreement Please read the following license agreement carefully.	Event Tracker
PRISM MICROSYSTEMS, INC. SOFTWARE LICENS	SE AGREEMENT
PLEASE READ THIS SOFTWARE LICENSE AGREE BEFORE DOWNLOADING, COPYING, OR USING TH	
BY CLICKING ON THE "ACCEPT" (OR EQUIVALENT BELOW, OPENING THE PACKAGE, DOWNLOADIN USING THE SOFTWARE, YOU ARE CONSENTING T TERMS AND CONDITIONS OF THIS AGREEMENT. I TO ALL OF THE TERMS OF THIS AGREEMENT, CLI	G, INSTALLING, OR TO BE BOUND BY THE F YOU DO NOT AGREE ICK THE "DECLINE" (OR
⊙ I accept the terms in the license agreement	Print
$\bigcirc$ I do not accept the terms in the license agreement	
InstallShield	
< Back	Next > Cancel
Figure 4: License Agreemen	t

- 4. Click the '**Next'** button.
- 5. Browse the certificate file, and then click the **Next >** button.

🛃 EventTrackerAgent 7.3	
Select a Certificate File Please provide a certificate file	Event Tracker
C:\Documents and Settings\deepa\Desktop\EventTracker	133998861 Browse
,	
InstallShield	
Figure 5: Select certific	Next > Cancel



6. In **Custom Setup**, there are two options: **EventTracker Windows Agent Only** and **Change Audit Agent Only**. (See Figure 6)

🙀 EventTrackerAgent 7.3	×	
Custom Setup           Select the program features you want installed.	Event Tracker 7	
Click on an icon in the list below to change how a feature is in	stalled.	
EventTracker Windows Agent Change Audit Agent	Feature Description Install only the Windows Agent component.	
	This feature requires approximately 12MB on your hard drive.	
Install to:		
C:\Program Files\Prism Microsystems\	Change	
InstallShield		
Help Space < Back	Next > Cancel	
Figure 6: Custom Setup		

Click evicent click clic

•	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 7			

• 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.
- 7. Click the **Change** button to change the installation path of the agent, and then click the **Next >** button. (See Figure 6).
- In the Event destination pane, enter the EventTracker manager name (Ex. Win2k3x64), Port number (Ex. 14580) and Change Audit manager name (Ex. Win2k3x64), and then click the Next > button (See Figure 8).



🛃 EventTrackerAgent 7.3	×
Configure Win XP/2003/Vista/2008 Events Destination	tTracker
Enter the system name where the Enterprise Event Manager is installed. Up to 5 managers can be configured separated by a comma $\langle_{\rm c}\rangle$	
EventTracker Manager: win2k3x64	
Port number: 14580	
Deploy SCAP Deploy WINSCP	
Enter the system/server name or IP address where the license certificate is	installed.
License Server: win2k3x4	
Port number: 14503	
Enter the name of the system where 'Change Audit Manager' is installed. If the standalone version, enter the local system name.	you want to install
Change Audit Manager: win2k3x64	
InstallShield	
< <u>B</u> ack <u>N</u> ext >	Cancel
Figure 8: Event Destination	

9. 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.

🔀 EventTrackerAgent	7.3	X
The wizard is rea	<b>the Program</b> dy to begin installation.	Event Tracker 🦻
Click Install to begin the i	nstallation.	
To review or change sett	ings,click Back. Cancel exits the w	izard.
🔲 Install default Remed	ial Action EXEs on this machine.	
Remedial Actions ( side, in response t		nched at either the Agent or Manager
	iger. These may be installed at the	aced in the EventTracker\Agent\Script e Agent side also, during deployment
InstallShield		
	< Back	Install Cancel
	Figure 9	



## 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.

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

Basic configuration		
<ul> <li>Network Connection Monitoring</li> <li>Connection Type</li> <li>TCP Open/Close</li> <li>UDP Open/Close</li> <li>Monitor</li> <li>All Network Traffic</li> <li>Only Suspicious Traffic</li> </ul> EventTracker includes several important features. You can customize EventTracker by enabling/disabling the above list of available features.		
ОК		

Figure 10: Basic Configuration



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





## Deployment through Group Policy

#### Before you Begin

 Modify Agent.ini and change EM (ENTERPRISE\_MANAGER), CM (Change Audit manager), InstallDIR (EventTracker Agent installation directory) EP (ENTERPRISE\_PORT), LS (License server name/ IP Address where the digital certificate is installed), and LP (License server port number) value appropriately.

[INSTALL_PATH][INSTALL_PATH]INSTALLDR= <installation agent="" be<br="" directory="" if="" need="" to=""></installation> installed in other than default path>INSTALLDR=[END][END][END][ENTERPRISE_MANAGER][EMTERPRISE_MANAGER]EM=Win2k3x64[EMD][ENTERPRISE_PORT][ENTERPRISE_PORT]EP=14580[END][END][END][CHANGEAUDIT_MANAGER][END][CHANGEAUDIT_MANAGER][END][CHANGEAUDIT_MANAGER][END][CHANGEAUDIT_MANAGER][END][CHANGEAUDIT_MANAGER][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1[RAT][END][END][DIGITAL_CERTIFICATE][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the number="" port="" server="">[END][END]LP=14503[LICENSE_SERVER_PORT][END]LP=[END]LP=DC=DEPLOY_SCAPI componentsDS=[DEPLOY_SCAP]Deploy SCAP components[DS=DPaloy WINSCP components[DS=Deploy SCAPI components[DS=DPALOY WINSCP components</the></the>	Configuration Settings	Sample Configuration
installed in other than default path>[END][END][ENTERPRISE_MANAGER][ENTERPRISE_MANAGER]EM=Win2k3x64EM= <eventtracker address="" hostname="" ip="" manager="" or="">[END][END][ENTERPRISE_PORT][END][ENTERPRISE_PORT][ENTERPRISE_PORT]EP=14580EP=<eventtracker enterprise="" number="" port="">[END][END][CHANGEAUDIT_MANAGER][CHANGEAUDIT_MANAGER]CM=Win2k3x64[CM=<change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1IR=1[END][END][DIGITAL_CERTIFICATE][DGITAL_CERTIFICATE]DC=DC = Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][LICENSE_SERVER_PORT][END][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]</license></the></change></eventtracker></eventtracker>		
[END][ENTERPRISE_MANAGER][ENTERPRISE_MANAGER]EM=Win2k3x64EM= <eventtracker address="" hostname="" ip="" manager="" or="">[END][END][ENTERPRISE_PORT][END]EP=14580EP=EventTracker Enterprise Port number&gt;[END][END][CHANGEAUDIT_MANAGER][END][CHANGEAUDIT_MANAGER][CM=<change address="" audit="" hostname="" ip="" manager="" or="">[END][END][CHEMEDIAL_ACTIONS][REMEDIAL_ACTIONS][R=1[R=1[END][END][DIGITAL_CERTIFICATE][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64[END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END][DEPLOY_SCAP]Deploy SCAPDS=[DEPLOY_SCAP][END]</license></the></change></eventtracker>		-
[ENTERPRISE_MANAGER]EM=Win2k3x64EM= <eventtracker address="" hostname="" ip="" manager="" or="">[END][END][ENTERPRISE_PORT][ENTERPRISE_PORT]EP=14580EP=<eventtracker enterprise="" number="" port="">[END][END][CHANGEAUDIT_MANAGER][CHANGEAUDIT_MANAGER]CM=Win2k3x64CM=<change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1IR=1[END][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][LNO]LP=14503[LICENSE_SERVER_PORT][END]LP=VAG03[LICENSE_SERVER_PORT][END]LP=14503[END]LP=14503[END]Deploy SCAP components[END]DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END][END][END]Deploy SCAP ComponentsDS=[DEPLOY_SCAP][END]</the></change></eventtracker></eventtracker>	•	
EM= <eventtracker address="" hostname="" ip="" manager="" or="">[END][END][ENTERPRISE_PORT][ENTERPRISE_PORT][ENTERPRISE_PORT]EP=14580EP=<eventtracker enterprise="" number="" port="">[END][END][CHANGEAUDIT_MANAGER][CHANGEAUDIT_MANAGER]CM=Vin2k3x64[CM=Change Audit Manager Hostname or IP Address&gt;[END][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1[R=1[END][IRD][DIGITAL_CERTIFICATE]DC=DC=DC= Certificate path and certificate name[END][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">[Deploy SCAP components[END][DEPLOY_SCAP][END][DEPLOY_SCAP]</license></the></eventtracker></eventtracker>		
[END][ENTERPRISE_PORT][ENTERPRISE_PORT]EP=14580EP= <eventtracker enterprise="" port_number="">[END][END][CHANGEAUDIT_MANAGER][CHANGEAUDIT_MANAGER]CM=Win2k3x64[CM=<change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1[REMEDIAL_ACTIONS]IR=1[IR][END][IDIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][LICENSE_SERVER_PORT][END][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END][DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]</license></the></change></eventtracker>		
ENTERPRISE_PORT]EP=14580EP= <eventtracker enterprise="" number="" port="">[END][END][CHANGEAUDIT_MANAGER][CHANGEAUDIT_MANAGER]CM=Win2k3x64CM=<change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1[END][DIGITAL_CERTIFICATE][DIGITAL_CERTIFICATE]DC=DC = Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][END]LP=14503[LICENSE_SERVER_PORT][END]LP=LENS_SERVER_PORT][END]LP=License server port number&gt;[DEPLOY_SCAP][END]DS=[DEPLOY_SCAP][END]</the></change></eventtracker>	5	
EP= <eventtracker enterprise="" number="" port="">[END][END][CHANGEAUDIT_MANAGER][CHANGEAUDIT_MANAGER]CM=Win2k3x64CM=<change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1IR=1[END][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DS=[DEPLOY_SCAP][END]DEPLOY_SCAP][END]</license></the></change></eventtracker>		
[END][CHANGEAUDIT_MANAGER][CHANGEAUDIT_MANAGER]CM=Win2k3x64CM= <change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1IR=1[END][END][DIGITAL_CERTIFICATE][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DS=[DEPLOY_SCAP][END]</license></the></change>		
[CHANGEAUDIT_MANAGER]CM=Win2k3x64CM= <change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1IR=1[END][END][DIGITAL_CERTIFICATE][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER][LICENSE_SERVER]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DS=[DEPLOY_SCAP][END]</license></the></change>		
CM= <change address="" audit="" hostname="" ip="" manager="" or="">[END][END][REMEDIAL_ACTIONS][REMEDIAL_ACTIONS]IR=1[R=1[END][END][DIGITAL_CERTIFICATE][DGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS=<the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DS=[DEPLOY_SCAP][END]</license></the></change>		
REMEDIAL_ACTIONS]IR=1IR=1[END][END][DIGITAL_CERTIFICATE][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DS=[DEPLOY_SCAP][END]</license></the>		[END]
IR=1[END][END][DIGITAL_CERTIFICATE][DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]Deploy SCAP components[DEPLOY_SCAP][END]</license></the>	[END]	[REMEDIAL_ACTIONS]
IEND]IEND][DIGITAL_CERTIFICATE]DC=[DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DEPLOY_SCAP]DEPLOY_SCAP][END]</license></the>	[REMEDIAL_ACTIONS]	IR=1
[DIGITAL_CERTIFICATE]DC=DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">[Deploy SCAP components[END]DS=[DEPLOY_SCAP][END]</license></the>	IR=1	[END]
DC= Certificate path and certificate name[END][END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">[END][END]Deploy SCAP components[END]DS=[DEPLOY_SCAP][END]</license></the>		
[END][LICENSE_SERVER][LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DS=DEPLOY_SCAP][END]</license></the>		
[LICENSE_SERVER]LS=Win2k3x64LS= <the address="" digital<="" ip="" name="" server="" td="" the="" where="">[END]certificate is installed&gt;[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP=<license number="" port="" server="">Deploy SCAP components[END]DEPLOY_SCAP]DEPLOY_SCAP][END]</license></the>		
LS= <the address="" digital<br="" ip="" name="" server="" the="" where=""></the> certificate is installed>[END][END][LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP= <license number="" port="" server="">Deploy SCAP components[END][DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]</license>		-
certificate is installed>[LICENSE_SERVER_PORT][END]LP=14503[LICENSE_SERVER_PORT][END]LP= <license number="" port="" server="">Deploy SCAP components[END][DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]</license>		
[END]LP=14503[LICENSE_SERVER_PORT][END]LP= <license number="" port="" server="">Deploy SCAP components[END][DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]</license>	0	
LICENSE_SERVER_PORT][END]LP= <license number="" port="" server="">Deploy SCAP components[END][DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]</license>		
LP= <license number="" port="" server="">Deploy SCAP components[END][DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]</license>		
[END][DEPLOY_SCAP]Deploy SCAP componentsDS=[DEPLOY_SCAP][END]		
Deploy SCAP componentsDS=[DEPLOY_SCAP][END]		
[DEPLOY_SCAP] [END]		-
	DS=	Deploy WINSCP components
[END] [DEPLOY_WINSCP]		
Deploy WINSCP components DW=		
[DEPLOY_WINSCP] [END]		
DW=		
[END]	[END]	

Table 1

- 2. Create a network share on server and allow **Domain Computers** to have at least **READ** access permission.
- 3. Copy the **AgentMSI\_73** folder to the network share, which is created in previous step.

Network share folder should have the below files. (See Figure 12)



Address 🗁 \\popeye\Shared\AgentMSI_73		
Name 🔺	Size	
💁 Agent.ini	2 KB	
Echange~1.cab	3,755 KB	
etwAgent73.exe	4,585 KB	
EventT~1.cab	10,939 KB	
EventTracker.cer	3 KB	
🔂 Event Tracker Agent. msi	19,812 KB	
🗐 ReadMe.txt	2 KB	
ڬ setup.bmp	589 KB	

Figure 12

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.

## 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)
- **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

- 1. Click Start >> Settings >> Control Panel >>, and then select Administrative Tools.
- 2. In Administrative Tools, click Group Policy Management.



Figure 13: 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.



🧟 Group Policy Management			
😹 File Action View Wind	🔜 File Action View Window Help		
🗢 🔿 🖄 🖬 🖉			
Group Policy Management A Forest: prismtest1.local B A Domains B A Domains B A Default Doma C Domain Contr	ollers	Domains Contents Domain prismtest1.local	
WMI Filters Starter GPO:	New Back Up All Manage Backups Open Migration Ta		
Group Policy Results	New Window from	Here	
	Refresh		
	Help		

Figure 14: Create Group Policy Object

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

New GPO		×
<u>N</u> ame:		
AgentMSI GP0		
Source Starter GPO:		
(none)		•
	ОК	Cancel
	Figure 15: New GPO	

4. Click the name of newly created GPO. In this case, 'AgentMSI GPO'.



🔜 Group Policy Management	
Eile Action View Window Help	
Group Policy Management Cross: prismtest I. local Cross: prismtest I. local prismtest I. local Crossing Default Domain Policy Crossing	
W SUBR2-SUL-Member-Server WS08R2-Web-Server WMI Filters	Security Filtering         The settings in this GPO can only apply to the following groups, users, and computers:         Name ^         Authenticated Users
	Add     Bemove     Properties
	WMI Filtering This GPD is linked to the following WMI filter: (none>

Figure 16

- 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.

Select User, Computer, or Group	? ×
Select this object type:	
User, Computer, Group, or Built-in security principal	<u>O</u> bject Types
Erom this location:	
Entire Directory	Locations
Enter the object name to select ( <u>examples</u> ):	
PRISMTEST1-VM2	<u>C</u> heck Names
	<b>_</b> (
Advanced OK	Cancel

Figure 17



- C. Click the **OK** button.
- 5. On the left hand side, right click on 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**.



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

🚞 Software Settings			
Software installation	Name	:	
	Sortware.	installation <u>N</u> ew ►	Package
		<u>P</u> aste Re <u>f</u> resh	
		Properties	
		Help	

Figure 19: Software Installation- create new package

6. An **Open** dialog box should appear.



Open						?	x
Look jn:	C AgentMSI_73			• 0	ø 🖻		
My Recent Documents Desktop My Documents My Computer	EventTrackerA	gent.msi					
My Network	File <u>n</u> ame:	EventTrackerAg	gent.msi		•	<u>O</u> pen	٦
Places	Files of <u>type</u> :	Windows Instal	ler packages (*.	.msi)	•	Cancel	

Figure 20

- A. Locate the UNC path of the server share where the MSI installer file is located (\\Server\Share\AgentMSI\_73\).
- B. Select the MSI installer file **EventTrackerAgent.msi**, and then click **Open**. EventTracker displays 'Deploy Software' dialog box.

Deploy Software	? ×
Select deployment method:	
C <u>Published</u> C <u>Assigned</u> C Ad <u>v</u> anced	
Select this option to Assign the ap	plication without modifications.
	OK Cancel

Figure 21: Deploy Software

- Select Assigned, and then click OK.
   You have now created and assigned the Package Object.
- 8. Right-click on the **Package Object**, and select **Properties**.
- 9. Click on the **Security** tab, and add **Domain Computers** to the security permissions.



EventTrackerAgent Properties		? ×
General Deployment Upgrades Categ	ories Modificatio	ons Security
Group or user names:		
CREATOR OWNER		<u> </u>
🖸 👧 Domain Admins (PCLOUD2003\Dom	nain Admins)	
Domain Computers (PCLOUD 2003\[		s)
Enterprise Admins (PCLOUD2003\E		
ENTERPRISE DOMAIN CONTROL		
	A <u>d</u> d	<u>R</u> emove
Permissions for Domain Computers	Allow	Deny
Full Control		
Read Assign	→ 🛛	
Write permission Special Permissions		H
		-
For special permissions or for advanced se	ettings,	Advanced
click Advanced.	L	Hatanood
	Cancel	
UK		<u>Apply</u>

Figure 22

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

10. Click the **Advanced** button, select **Domain Computers**, and then click **Edit**.



Permissions	nore information about special permi	rmissions		click Edit.	? X
Туре	Name	Permission	Inherited From		
Allow	Authenticated Users	Constant	And the factor and the state		
Allow	Domain Admins (PCLOUD2003.	Permission Entry	for d3efe649-00a6	-49b0-afc4	-abeef7 <mark>?</mark> 🗙
Allow	Domain Computers (PCLOUD2.				
Allow	SYSTEM	Object Propertie:	sl		
Allow	Authenticated Users				1
Allow	CREATOR OWNER				
Allow	Domain Admins (PCLOUD2003.	<u>Name: ters (PC</u>	LOUD2003\Domain 0	Computers]	Change
Allow	Enterprise Admins (PCLOUD20.				
- A 11	ENTERPRICE ROUMIN CON	Apply onto: Thi	s object only		<b>T</b>
Ade	d Edit				_
A		Permissions:		Allow	Deny
To replace	inheritable permissions from the pa with entries explicitly defined here e all permission entries with the de e about <u>access control</u> .	Full Control List Contents Read All Prop Write All Prop Delete Read Permiss Modify Permis All Validated V	erties ions sions		
		Apply these p containers wi	ermissions to objects thin this container only	and/or	Cjear All
			[	OK	Cancel

Figure 23: Assign permissions

Check the List Contents, Read All Properties, and Read Permissions options, if not selected.

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



Active Directory Users and Composite Compos				
•	- 19 🖻 😫 19   🦉 🖉 💩 1	7 🍕 🙍		
Active Directory Users and Computer	GROUP policy 2 objects			
⊡ Saved Queries ⊡∰ PCLOUD2003.com	Name V	Туре	Description	
🛱 🧰 Builtin	PRISM-4E7F60F03 PCLOUD69-VM1	Computer Computer		
Computers     Computers     Computers     Comparison Controllers     Comparison Controlers     Comparison Controlers     Comparison Controllers     Com		Compace		

#### Figure 24: Create new OU

- 12. In the **New Organizational Unit** has to be created .For example: Group policy.
- 13. Right click newly created OU, and then click Link an Existing GPO.

Figure Group Policy Management	_ 🗆 🗵
්දී Eile Action View Window Help	_8×
Group Policy Management Forest: PCLOUD2003.com Domains PCLOUD2003.com PCLOUD2005.com PCLOUD2003.com PCLOUD2005.com PCLO	 WMI Fit None
Group Policy Results	

Figure 25: Link an existing GPO



- 14. In the **Select GPO** dialog box, select the appropriate **domain name** and newly created **Group Policy Object**, and then click the **OK** button.
- 15. Close the **Group Policy window**.

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

16. Force replication to all other domain controllers.

## NOTE:

EventTracker/Change Audit agents will be installed once the target machines are restarted.



## Verifying 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 Pre-Vista Operating System:

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 Vista and Post-Vista Operating System:

#### 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

## Manual Agent Installation [Batch File Install]

#### EventTracker Agent Installation

#### A. <u>Prepare the files for manual agent install (EventTracker Agent)</u>

- 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\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\ AlTemp\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

- 1) Execute install.bat.
- C. Perform 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.

#### D. Perform the installation on 64 bit OS

- 1) Open the file Agent\etsetup.ins and update "INSTALLPATH=\Program Files (x86)\Prism Microsystems\EventTracker\Agent".
- 2) Execute installx64.bat (follow steps "C" if UAC is enabled).

#### Change Audit Agent Installation

#### A. Prepare the files for manual agent install (EventTracker 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
- 1) Execute install.bat.
- C. Perform 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.



#### D. Perform 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 (follow steps "C" if UAC is enabled).

### 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.

