# Netsurion. EventTracker\*

# EventTracker Upgrade Guide Upgrade to v9.3

Publication Date: July 24, 2020

# Abstract

The purpose of this document is to help the existing users of EventTracker to upgrade to a newer version and to verify the expected functionality and performance of all its components.

## Audience

It is incumbent upon all users of EventTracker v9.0/v9.1/v9.2 who want to upgrade to EventTracker v9.3.





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.	In	trodu	uction	4
	1.1	Upg	grade Requirements	4
	1.	1.1	Software Requirements	4
	1.	1.2	Preparations for the upgrade	5
	1.2	Pre	requisites	6
	1.3	Plar	nning	7
2.	Up	pgrac	de - Quick View	7
	2.1	Con	nmon steps for all upgrades	7
	2.	1.1	Pre-upgrade process	7
	2.	1.2	Post-upgrade process	8
	2.2	Upg	grading to EventTracker v9.3	8
3.	Up	pgrac	de - Detailed View	.1
	3.1	Upg	grade from v9.0/v9.1/v9.2 to v9.3 1	.1
	3.2	Con	figuring Service Accounts	\$5
4.	So	ource	Type Mapping	;9



# 1. Introduction

This guide describes about upgrading EventTracker. It is strongly recommended that you read the entire document thoroughly before you begin the upgrade process. EventTracker v9.3 upgrade will only support Operating systems Windows Server 2012 R2, Windows 10, Windows Server 2016, and Windows Server 2019.

For the user's convenience, this guide is separated into two parts: 'Upgrade- Quick View' and 'Upgrade-Detailed View'.

**Upgrade - Quick View** is written for the system administrators and the experts familiar with EventTracker and the upgrade process. It is presumed that the user of this section has enough knowledge of the system and configuration process.

**Upgrade** - **Detailed View** is meant for EventTracker users upgrading EventTracker for the first time. In this section, the upgrade process is explained with the help of GUI (Graphical User Interface).

#### NOTE:

- It is recommended not to install/upgrade EventTracker in a Domain Controller.
- It is recommended to run the EventTracker Manager Console on a Dedicated Windows Server.

## 1.1 Upgrade Requirements

- The software requirements
- Preparations for the upgrade

#### 1.1.1 Software Requirements

#### EventTracker Manager

Microsoft Windows Platforms	64 bit	Upgrade
Server 2019	Supported	Supported
Windows 10	Supported	Supported
Server 2012 R2	Supported	Supported
Server 2016	Supported	Supported



SQL server	64 bit
SQL Server 2017	Supported
SQL Server 2016	Supported

#### EventTracker Agent

Microsoft Windows Platforms	32 bit	64 bit
Server 2019	Not Applicable	Supported
Windows 10	Supported	Supported
Windows 8, 8.1	Supported	Supported
Windows 7	Supported	Supported
Server 2008	Supported	Supported
Server 2008 R2	Not Applicable	Supported
Server 2012	Not Applicable	Supported
Server 2012 R2	Not Applicable	Supported
Server 2016	Not Applicable	Supported
EventTracker Ag	ent for Solaris: Solaris	9, Solaris 10
Microsoft Windows 7 E	mbedded and Micros Enterprise	oft Windows 10 IOT

#### Components

• Microsoft .NET Framework 3.5 and above.

**NOTE:** Versions other than those specified above are not supported.

#### 1.1.2 Preparations for the upgrade

1. Thoroughly read the 'EventTracker Architecture' guide. This guide explains the architecture and sample deployment methods with illustrations.

Managing Billions of Logs Everyday.



- 2. Contact <a href="mailto:support@eventtracker.com">support@eventtracker.com</a> for information regarding license keys or license certificates.
- 3. If you have installed an earlier version of EventTracker using IIS Express, before upgrading please change it to IIS to proceed with the installation.
- 4. While upgrading from v9.0/v9.1/v9.2 to v9.3, only SQL 2016 and 2017 (both Express and Enterprise) are supported. SQL Upgrade Link:

https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-2017

#### **IMPORTANT:**

• Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path (Eg.Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceType Mapping.exe)

*Kindly refer the <u>Source Type Mapping</u> section to install the same.* 

- After upgrading the Collection Master, the user may notice the inconsistency in Reports/ Log Search/Cab received status (Admin>Collection Master>Archives status) until the database migration is completed.
- After upgrading the Collection Point, the user may not be able to view the exact cab transfer status in (Admin>Collection Point Configuration-> manage archives) until the database migration is completed.

#### RECOMMENDED

- Any user(s) on EventTracker version below v9.0 needs to upgrade to v9.0/v9.1/v9.2 first and then upgrade to v9.3.
- Any user(s) on EventTracker version v9.0/v9.1/v9.2 can upgrade to v9.3

### 1.2 Prerequisites

Before you begin with the upgrade process, please follow this checklist and ensure that you have all the components in place to perform a successful upgrade.

- Ensure Windows updates with all the latest service packs are installed.
- The most effective upgrade method is to first export all the custom settings using Export Import Utility, install the new version, and then import the custom settings. There is no need to export all policy settings since all the categories included in any prior versions have been retained.



• The recommended method is to first upgrade the Manager and validate all its functionality. Then proceed with upgrade of the Agents and lastly verify the performance.

## 1.3 Planning

This section gives an estimated time required for the upgrade and monitor the successful upgrade. It may take 60 – 90 minutes for you to read this document and to complete the upgrade process. It is required to spend some time to verify all the 'Scheduled Reports' being generated.

# 2. Upgrade - Quick View

In this section, you can get a quick insight into the upgrade process

- <u>Common steps for all upgrades</u>
- Upgrade from v9.0/v9.1/v9.2 to v9.3

## 2.1 Common steps for all upgrades

### 2.1.1 Pre-upgrade process

- Verify that all the prerequisites have been satisfied.
- Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path (Eg.Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceT ypeMapping.exe) Kindly refer the <u>Source Type Mapping</u> section to install the same.
- Before you start the upgrade process, please take a backup of the integrator folder present in the manager agent installed location (Install path\Prism Microsystems\EventTracker\Agent). Please ensure to disable all the integrator related tasks from the windows task scheduler.
- For v9.0, v9.1 and v9.2, you can take a backup of the database from EventTracker Control Panel > Diagnostics which is explained in detail in Upgrade from v9.0/v9.1/v9.2 to v9.3
- If you have incorporated your company logo into EventTracker, then take a backup of the .jpg file of your company logo before uninstalling the EventTracker. You need to replace the backed up image file after installing EventTracker.
- For CM and CP set up, please upgrade CM (Collection Master) first, and then upgrade CP (Collection point).



**NOTE:** While upgrading from EventTracker v9.0/v9.1/v9.2 to v9.3, if the environment consists of supported SQL server (SQL 2016 or SQL 2017), then the user needs to configure the SQL services to the network services manually.

• To change the configuration from SQL services to the network, open the run command and type in services.msc and click **ok**.

In the services page, right click the **SQL Server** service and click properties. In the properties window, click the **Log on** tab, select **This account** option and click **Browse**. Select the entire directory option and click **ok**.

• The logged-in user who is upgrading to EventTracker v9.3 should have SQL sysadmin privilege. If the user does not have enough permission, then an error message appears.

Select SQ	L Instance 🛛 🔀
?	Currently logged in user and the system's administrator group do not have necessary permissions on SQL Instance '.\EVENTTRACKER'. Please make sure the logged in user is having sysadmin permission on the SQL Instance '.\EVENTTRACKER' before continuing the installation. Do you want to continue?
	<u>Yes</u> <u>N</u> o



- Backup all Custom Categories, Alerts (Please check the 'Export E-mail Settings' check box), Filters and Reports using Export Import Utility.
- Please note the custom changes made in the 'Trusted List' (Agent Configuration -> Network Connection Monitor -> Suspicious Traffic Only (SNAM) -> Trusted List).

### 2.1.2 Post-upgrade process

- If SSL (HTTPS) is configured in the earlier version, then the configuration will not be retained after the upgrade to v9.3. Ensure to reconfigure it as mentioned in <u>Securing IIS Web Server with SSL</u>.
- If the user has configured the JSON file in DLA Manager in the older version, after upgrading, the user will have to reconfigure the same.

# 2.2 Upgrading to EventTracker v9.3

1. Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path



(Eg.Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceT ypeMapping.exe)

Kindly refer the <u>Source Type Mapping</u> section to install the same.

- Before you start the upgrade process, please take a backup of the integrator folder present in the manager agent installed location (Install path\Prism Microsystems\EventTracker\Agent). Please ensure to disable all the integrator related tasks from the windows task scheduler.
- 3. Uninstall the existing version by retaining old configuration and data.
- 4. Restart the EventTracker manager server or system.
- 5. Install EventTracker v9.3. Click Yes to proceed with upgrade.

EventTracker Pre-Install Check	×
Previous installation configuration configur	on has been detected, would you like to
	Yes No



- 6. <u>Configure the service accounts</u>, if the archives/reports are stored in the network path.
- 7. Update the Trusted List with the changes you have noted down earlier.
- 8. Upgrade all windows agents using 'System Manager'.
- Preferred: Import the latest knowledge objects (KO) after upgrading from v9.0 /v9.1 to v9.3. The newly optimized knowledge objects contain improvements in RegEx matching and source type mapping. Refer to the User Guide and knowledge object portal for more information on knowledge objects.

Note:

- Please import EventTracker and Windows KOs on top of existing KO.
- Please delete any other KOs and import the new KOs as per the need.
- If new KOs are not imported, only standard properties will be indexed.
- 10. After upgrading to EventTracker v9.3, copy the backed-up integrator folder in the manager agent installed location (Install path\Prism Microsystems\EventTracker\Agent). Start all the integrator tasks from the windows task scheduler to receive the integrator data.

# Netsurion. EventTracker

Netsurion. | EventTracker

11. **Optional:** To utilize newly added/Modified categories/alerts, import the complete alerts /complete categories files from the configuration directory (Install directory). Prior to importing, user needs to manually delete existing categories and alerts from the application. Then import all categories and all alerts from configuration files.

#### **Compliance Dashboard**

• The Dashlets created under **Compliance dashboard** are preserved after the upgrade and the user can customize the dashlets by selecting the customize icon **S**.

$\equiv$			Admin		💽 Sunanda Das 👻
	Correction or	Customize dashlets	×		
	Compliance			<b>m</b> / U	ashboard / Compliance
Q	Dashboard new sa	Lucene_Upgrade Unknown Process1		+ 0	9 <b>* 1</b> T 9
×					
		Add Dele	ete Close		



#### My Dashboard

• The dashlets created under **My Dashboard** are preserved after the upgrade and the user can customize the dashlets by selecting the customize icon **O**.

My Dashboard						🕈 / Dashboard / My Dashboard
Dashboard						0 0 🖓 🌣 🖻 1 🏾 0 0
	Customize dashlets				×	
Г				<b>D</b> .44		
L	Log Volume report	Lucene_upgrade	Unknown Processi		_	
				Add	Delete Close	

Figure 4



# 3. Upgrade - Detailed View

In this section, you will learn the upgrade process in detail.

## 3.1 Upgrade from v9.0/v9.1/v9.2 to v9.3

- 1. Please refer to the <u>Common steps for all upgrades</u> for more details.
- 2. Before upgrading, please take a backup of the database and details are given below.
  - a. Double-click EventTracker Control Panel, double-click Diagnostics.
  - b. Click the Backup Configuration button. Backup & Restore window displays.

Backup & Restore	×
🕞 🖲 Backup	
Backup to Browse	
Maximum number of backup files 64	
Backup now as read only	
Schedule	
Scheduled backup	
▼ at 0 - : 0 - hrs	
on 🔽	
Restore from Browse	
Save Restore Close	

Figure 5

- c. Browse and select the folder you want to back up.
- d. Click the Backup now button.
- e. After the backup is taken, navigate to the backed up folder. A file with the extension .bkp is used to restore later.
- Before you start the upgrade process, please take a backup of the integrator folder present in the manager agent installed location (Install path\Prism Microsystems\EventTracker\Agent). Please ensure to disable all the integrator related tasks from the windows task scheduler.

#### Step 1: Close/terminate all the EventTracker Components

Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path (Eg.Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceType Mapping.exe)

#### Kindly refer the <u>Source Type Mapping</u> section to install the same

- Before you start with the upgrade, it is important to close/terminate all the EventTracker components present in the system, like EventTracker, EventTracker Control Panel, and even **RDP** (Remote Desktop Protocol) session.
- During uninstall, if any of the previous EventTracker components is open then EventTracker prompts you to close the program.
- Close the open component, and then click the **Retry** button. EventTracker resumes the uninstall process.

#### Step 2: Uninstall v9.0/v9.1/v9.2

- 1. Click Start, select Settings, and then select Control Panel.
- 2. Select Add or Remove Programs, select EventTracker, and then click Remove.

#### (OR)

Click **Start**, select **Programs**, and then select **Prism Microsystems**. Select **EventTracker**, and then click **Uninstall EventTracker**. EventTracker will display the confirmation message.



Figure 6

3. If you have installed EventTracker agents on different systems then a message box will appear to confirm the uninstall process.



EventTra	acker 🛛 🔀
2	You have installed EventTracker Agents on several systems and not uninstalled them yet. It is recommended that you uninstall these agents before uninstalling the manager. Do you want to continue with this uninstallation?
	Yes No



Click Yes to continue the installation process.
 EventTracker starts the uninstall process, and displays 'Uninstall EventTracker' dialog box.



#### Uninstall EventTracker' dialog box for EventTracker v9.1

Figure 8

Netsurion. EventTracker

Uninstall EventTracker' dialog box for EventTracker v9.0/v9.2





By default, all the file options are selected. Keep the default selection to retain the data and configurations.

5. Click **Ok**.

#### Step 3: Restart the EventTracker Manager Server or System

- 1. Close all the open applications on the desktop.
- 2. Click Start and then click Shut Down dropdown.
- 3. Select the **Restart** option, and then click **OK**.

#### Step 4: Install EventTracker v9.3

Kindly follow the steps mentioned below for the upgrade process.

1. Double-click the executable file.

**NOTE**: .NET 4.8. is enabled by default for Microsoft Windows 2012 R2/2016/10/2019. If it is not available, EventTracker pre-install check will install .NET 4.8.

EventTracker		$\times$
EventTracker 9.2 requires .NET Framework Quit	: 4.8. Click Yes to Install, No to	þ
	Yes No	

Figure 10



IMPORTANT: In Internet Explorer->Browser Settings->Security->Custom Level-> In the downloads->File Download-> Please make sure "enable" option is selected.

WICHOSOIC INCL'I Harrework	
NET Framework 4.8 Setup Please wait while the .NET Framework is being installed.	.NI
Download progress:	
Downloading Windows10.0-KB4486153-x64.cab	
Installation progress:	<u> </u>
Installation progress:	े
Installation progress:	C
Installation progress:	<u> </u>
Installation progress:	<u> </u>
Installation progress:	0
Installation progress:	0



2. Once the .net framework 4.8 is installed a message pop's up, click ok and reboot manually.

EventTracker	2
A reboot is required to continue of Please reboot and launch the Eve	with installation. ntTracker setup again to continue.



3. After the reboot relaunch the EventTracker setup.



Figure 13

EventTracker Pre-Install Check window opens.



EventTracker Pre-Instal	l Check
	Netsurion. EventTracker
Welcome	Welcome to EventTracker Pre-Install check
License	
Hardware Summary	
Install Type	
Prerequisite	24/7
Install	
Define User Group	
Define User	
Summary	RESPOND
	This application helps the Administrators to validate their environment and assess if it is ready for EventTracker installation. Checks hardware for minimum requirements Checks for network connectivity Checks prerequistes and offers to install them Checks for configuration of users and offers them to create the configuration Both on screen and text reports are provided which can help for further troubleshooting
Quit	Next >

Figure 14

4. Click **Next**. License page opens.

ventTracker Pre-Insta	ll Check	2
	Netsurion. EventTracker	
	License Agreement	
Welcome	Please read the following license agreement carefully.	
License		
Hardware Summary	EVENTTRACKER SECURITY LLC END USER SOFTWARE LICENSE AGREEMENT	1
Install Type	NOTICE - THIS END USER LICENSE AGREEMENT ("EULA" OR "AGREEMENT") IS A LEGAL DOCUMENT BETWEEN	l
Prerequisite	EVENTTRACKER SECURITY LLC. ("EVENTTRACKER" OR "LICENSOR") AND THE LEGAL ENTITY THAT ACQUIRED THE EVENTTRACKER SOFTWARE FOR USE BY AN END USER ("YOU", "YOUR", "CUSTOMER" AND "LICENSEE").	
Install	READ THIS BEFORE INSTALLING. USING OR OTHERWISE ACCESSING EVENTTRACKER'S PROPRIETARY SOFTWARE.	
Define User Group	INCLUDING SOFTWARE AS A SERVICE, TRIAL OR EVALUATION AND ACCOMPANYING DOCUMENTATION (the "SOFTWARE").	
Define User	THE SOFTWARE IS COPYRIGHTED AND IS LICENSED, NOT SOLD, TO YOU BY EVENTTRACKER. BY CLICKING ON THE	
Summary	ACCEP 1" (OR EQUIVALENT) BUTTON OR SIGNING BELOW, OPENING THE PACKAGE, DOWNLOADING, INSTALLING, USING OF OTHERWISE ACCESSING THE SOFTWARE. INDICATES THAT YOU HAVE READ. UNDERSTAND, ACCEPT, AGREE TO BE	1
	BOUND BY THE TERMS AND CONDITIONS, AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THE LEGAL ENTITY. IF AT ANY TIME YOU DO NOT ACCEPT THESE TERMS, YOU MUST IMMEDIATELY DELETE THE SOFTWARE AND CEASE USING OR ACCESSING THE SOFTWARE.	:
	1. License Grant Subject to the terms of this Agreement, including payment of applicable fees, you have a non-exclusive and nontransferable right to use the Software for non-commercial (e.g. not for resale or rental or the like) or evaluation purposes, and only for the permitted number of servers, network devices or workstations as designated in the applicable Statement of Work (SOW), Work Order or Purchase Order (Hereinaffer Order) and for the term designated in the applicable Order between Event Tracker and Customer or between Customer and authorized Event Tracker partners. All Orders shall incorporate this agreement by reference. The term Software shall include any updates, additions or	•
Quit	< Back Accept	

Figure 15

5. Click Next.

Hardware Summary pane opens.

#### NOTE:

It may take a few seconds to fetch the hardware details and a processing symbol will appear during the data collection process.



EventTracker Pre-Install C	heck		×
		Netsurion. EventTracker	
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group Define User Summary	Machine Name IP Address MAC Address Processor RAM Network Connectivity OS Version Disk space	N <sup>3</sup> 1: 34 94 :E 1 CPU x 4 Core(s) 7.91 GB ☑ Ok Microsoft Windows 10 Pro C: Total 300 GB, Free 238 GB D: Total 630 GB, Free 629 GB	
Quit		< Back	Next >

Figure 16

6. Click **Next**. Prerequisite page opens.

EventTracker Pre-Install Check			
Netsurion EventTracker*			
Wolcomo	Prerequisites that	are needed:	
License Hardware Summary	N	Microsoft .NET Framework (4.8.03761)	Installed
Install Type	Microsoft	IIS (Version 8.5)	Installed
Install		Windows Installer (5.0)	Installed
Define User		SQL ODBC Driver (12.2.5543.11)	Installed
Summary	$\mathbf{\Sigma}$	PowerShell (5.1.14409.1005)	Installed
	=	Easticsearch (7.2.1)	Not Installed
	SQL Server	Microsoft SQL Server 2017 Express Edition (14.0.1000.169)	Installed
Quit	·	< Back	Next >

Figure 17

#### NOTE:

• If the prerequisites are not installed, then a message '**Not-Installed**' displays against the respective prerequisite.



• If the Elasticsearch (7.2.1) is not installed the following message pop's up.

"Upgrade from v9.0/v9.1 to v9.3, EventTracker old Elasticsearch index data will be deleted".

EventTracker Pre-Install Check		
	Netsurion. EventTracker	
Welcome	Prerequisites that are needed:	
License Hardware Summary	Microsoft .NET Framework (4.8.03761)	
Install Type Prerequisite	EventTracker Pre-Install Check	
Install Define User Group Define User	During upgrade to v9.3, EventTracker old Elasticsearch index data will be deleted.	
Summary	С ОК саled	
	Elasticsearch (7.2.1) Not Installed	
	Microsoft SQL Server 2017 Express Edition (14.0.1000.169) Installed	ļ
Quit	< Back Next	>

Figure 18

7. Click **OK** to proceed.

EventTracker Pre-Install Check x		
	Netsurion. EventTracker	
Welcome License Hardware Summary Install Type Prerequisite <b>Install</b> Define User Group Define User Summary	[ Downloading Elasticsearch ] 10 MB downloaded out of 248 MB, 4% complete Note: In case the installer prompts for a restart/reboot of the system, please do so. Failing to do so, might make the system unusable. Once that is done please run this setup again. View Details	
Quit	< Back	Next >

Figure 19



- 8. Click **Next** and the **summary** page opens. In **Summary** page, verify all the data entered and then click **Install**.
- 9. Click Install to proceed with the installation.

EventTracker Pre-Install Check EventTracker*			
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group Define User	Event Tracker Archive Drive Event Tracker Program Drive Elasticsearch Data Drive Elasticsearch Network Adapters Operating System Version Hard Disk Summary	C:\Program Files (x86)       vent Tracker\Archives         C:\Program Files (x86)\Prism Microsystems\Event Tracker\Cache         Elasticsearch (7.2.1)(Installed)         172.3       3         Microsoft Windows Server 2016 Datacenter         C: Total 299 GB, Free 274 GB	
Summary	EventTracker User Group EventTracker Administrator User Internet Information Services Microsoft SQL Server Please check : [C:\EventTracker	G-Event Tracker-Testing  I I IIS[Version 10.0] (Installed)  Microsoft SQL Server 2017 Express Edition(Installed)  Preinstall-Check_000C29528468.log] for more details.	×
<u>Q</u> uit		< <u>B</u> ack	Install

Figure 20

EventTracker - Install Shield Wizard opens.





Figure 21

EventTracker - InstallShield Wizard displays the **Welcome** screen.

還 EventTracker 9.3	×
	Netsurion. EventTracker
	Welcome to EventTracker Setup Program.
	This setup program will install EventTracker on your computer. To continue, click Next.
	WARNING: This program is protected by copyright law and international treaties.
	Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
	© Copyright 2020 EventTracker, All Rights Reserved
	<back next=""> Cancel</back>

Figure 22

 Select a Certificate File
 Netsurion.
 EventTracker

 Please provide a certificate file
 Netsurion.
 EventTracker

 Browse...
 Browse...

10. Click Next. Select a Certificate File page opens.



- 11. Click **Browse** to locate the path of the certificate file.
- 12. Select File window opens. Go to the appropriate folder, select File and then click Open.

The folder path is updated.

🔀 EventTracker 9.3			×
Select a Certificate File			9
Please provide a certificate file		Netsurion.	ventiracker
\192.168.1.7\Test-Documents\9.)	(_CE		Browse
InstallShield			
	< Back	Next >	Cancel

Figure 24



13. Click Next . Select Components screen opens.

🔀 EventTracker 9.3	×
Select Components Select EventTracker components from the options below.	Netsurion. EventTracker
Click on an icon in the list below to change how a feature is ins	stalled. Feature Description Complete framework capable of log management, change audit.
	This feature requires 9102KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 483MB on your hard drive.
Install to: C:\Program Files (x86)\Prism Microsystems\ InstallShield	Change
Help Space < Back	Next > Cancel

#### Figure 25

EventTracker Components	Description
EventTracker Console	Select this option to install the manager console on target the computer.
Change Audit	Optional component. Installing this component enables you to monitor and manage change over the enterprise. The agent component will also be installed along with the Manager Console. You can also deploy the agent to the monitored computers using System Manager after installing the Manager Console.
Trap Tracker	Optional component. Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.

#### 14. Click Next.

InstallShield Wizard displays the **Select EventTracker Console Type** screen. It opens the previously selected option in version 9.0 or 9.1 or 9.2 by default.





Figure 26

#### 15. Click Next.

The **Ready to Install the Program screen** displays the summary of the installation path, console type, and the selected features.

🛃 EventTracker 9.3	×
Ready to install the Program	0
The wizard is ready to begin installation.	Netsurion. EventTracker'
Click Install to begin the installation.	
Installation Path: C: \Program Files (x86) \Prism Microsystems\	
Console Type: Standard	
<b>List of selected features:</b> EventTracker Change Audit TrapTracker	
To review or change settings, click Back. Cancel exits the	wizard.
InstallShield	
< Back	Install Cancel

Figure 27

#### 16. Click Install.

InstallShield Wizard installs the selected components.

InstallShield Wizard displays the last screen.





Figure 28

17. Click **Finish** to conclude the installation process. InstallShield Wizard displays the **EventTracker Configuration** screen.

i e	ventTracker :: Configuration		×
Ne	tsurion EventTra	cker	
Use	er Credentials	User Authentication	
	User Name NTPL'	Local Account	
	Password [********	Active Directory	
Eve	entTracker Group G-EventTracker-Te	Database Authentication	
Note For % doma name	r Active Directory" authentication enter in user and for "Local Account" auther and password. User must be adminis	OK Cancel user name and password of a tication enter local system user trator on this system. Refer install quide.	



• Type valid user credentials in the User Name and Password fields respectively and then click OK. After successfully validating the user credentials, InstallShield[R] Wizard opens the EventTracker Configuration message box.





Figure 30

#### 18. Click **OK**.

#### Step 5: Configure the service accounts, if the archives/reports are stored in the network path.

Click '<u>Configure the service accounts</u>' section.

#### Step 6: Verify that the Categories, Alerts, Filters, are intact.

**Step 7:** After upgrading to EventTracker v9.3, copy the backed-up integrator folder in the manager agent installed location (**Install path\Prism Microsystems\EventTracker\Agent)**. Start all the integrator tasks from the windows task scheduler to receive the integrator data.

#### Step 8: Upgrade all Windows agents using the System manager

EventTracker agent upgrade is necessary to keep the agents up to date with the manager system.

- 1. Logon to **EventTracker**.
- 2. Select the Admin menu and select Systems. EventTracker opens System manager page.
- 3. Click the desired domain/group name and then select the **Upgrade agent**.

Systems						🔒 / Admi	in / Syste
2	0		8	Managed	3	9.0 - Build 18 1 9.1 - Build 19 1 9.2 - Build 19 1	
Non Reporting Systems Systems not reporting since the last 24 hours	Details Edit Move systems	st Status Fvarious sensor requests	Managed v Managed/Unm	s Unmanaged anaged system count	EventTracker Se Version by count	nsor Version	
< Groups	Install agent/Start poll Uninstall agent/Stop poll						
Create Group Delete Group	Upgrade agent Restart agent service	Non Reporting Systems Search Compute	rs System Report Aut	to Discover C		(a) Managed	: 7
	Query for agent version	101053			Page size	Sort by columns	
Search Groups	C Remove agent components Delete systems Manage asset value	Q.			25	Computer	~
All Groups	Query for agent update info	of 1 > GO					
Domain Controllers	Computer		Type Port	EventTracker version	Change audit version	Asset value	
EventTracker	o		Unknown 14605	9.1 - Build 19		Undefined	\$
Firewall Devices	OLA DLA		2008 R2 14 2			Undefined	\$
Network Devices	PLD1 ILR38	DLN	Win 7 14 5	9.0 - Build 18		Low	\$
TTELTINES STUTION			2010 14505	0.0 0.001	0.0 0.0117	Contract of the second s	3%



Netsurion. EventTracker<sup>®</sup>

EventTracker displays Upgrade Remote Agent(s) dialog box.

Upgrade Remote agent(s)						×
Select systems and agent type						
All systems in the selected group						
○ Take systems from text file	Browse					
(One system per line)						
Agent Type 🗌 EventTracker 🛛 Change Audit						
O Specific systems in the selected group						
		Consul	Peels	Neut	Advanced	Unereda
		Cancel	Back	ivext	Advanced	Upgrade

Figure 32

Option	То
All systems in the selected group	Click this option to upgrade all the agents in the selected group.
Take systems from the text file	Create a text file containing agent system names for which the upgrade has to be done. The text file should contain one system name per line. If you select this option, then browse the text file to select the agent system names.
Agent type	Select the agent to upgrade.
Specific systems in the selected group	Out of all the agent systems present in the group, select a specific agent system(s) to upgrade.

#### (OR)

Click the Gear corresponding to the remote system's name (where the agent is to be upgraded), and then click **Upgrade Agent** from the dropdown list.



🕈 / Admin / Syster

Systems

2 Non Reporting Systems Systems not reporting since the last 24 hours	O Request Status Status of various sensor requests	8 Managed Managed vs Unmanaged Managed/Unmanaged system count	EventTracke	9.0 - Ruie 18 1 9.1 - Ruie 19 1 9.2 - Ruie 7 1 r Sensor Version
Groups Create Group Delete Group	Systems Request Status Non Reporting Systems Search Com	puters System Report Auto Discover C		
Image: Constraint of the second sec	All Domain Computers Type here	Q	Page size	Managed: 7     Sort by columns     Details
All Groups O Default O	Computer	Type Port EventTracker v	rsion Change audit version	Install agent/Start poll Uninstall agent/Stop poll Manage asset value Upgrade agent
Demain Controllers EventTacker Firewall Devices Network Devices VimWare Win 7 and Server 2008 Above	7 741 LR14 7 741 LRX 7 741 LRX 6 55 411- 4	Unknown         14         5         9.1 - Build 19           2008 R2         14         2            Win 7         14         5         9.0 - Build 18           2016         14         5         9.2 - Build 7           2016         14         5	  9.2 - Build 7 	Remove agent components Restart agent service Agent service status Query for agent version Query for agent update info Enable systog relay



EventTracker displays Upgrade Remote agent(s) pop-up window.

Jpgrade Remote agent(s)						×
Agent(s) will be up	ograded on the foll	owing remote computer(s).				
Name	EventTracker	,				
NTOLOTOLO14						
		Select "Next" to proceed.				
			Cancel	Back Next	Advanced	Upgrade



# Netsurion. EventTracker

4. Check the agent type option which you want to upgrade, and then click **Next**.

Jpgrade Remote agent(s)	)			×
Agent(s) will be up	ograded on the fol	lowing remote computer(s).		
Name	EventTracke	r		
MITEDIDENTA	$\checkmark$			
		Select "Next" to proceed.		
			Cancel Back Next Ad	vanced Upgrade

Figure 35

5. Select the Windows Domain Network option, and fill in the user credentials.

	(s)				
elect the method	l of upgrade.				
Windows Domain Network	twork				
Account	tonns\s	(ex. mydomain\administrato	r)		
Password	•••••				
Confirm Password	•••••				
Choose 'Upgrade C	Vver IP' option to upgrade the agen	t which is outside the domain.			
Deploy WinSCP					
Deploy WinSCP     Install default Remed	ial Action EXEs on this system 🛈				
Deploy WinSCP Install default Remed EventTracker :	ial Action EXEs on this system ①				
Deploy WinSCP Install default Remed EventTracker :	ial Action EXEs on this system 🛈	Select "Upgrade" to proceed.			

Figure 36

(OR)



If the remote agent is in some other non-trusted domain or the remote system is not accessible using Windows file sharing, then select the **Upgrade over IP (Non-Windows Domain)** option.

Upgrade Remote agent	(5)							×
Select the method	of upgrade.							^
Windows Domain Net	twork							1
Account	tonns\si "	(ex. mydomain\administrator)						
Password	•••••							
Confirm Password	•••••							
Upgrade over IP (Nor	n Windows Domain)							
Choose "Upgrade C	Iver IP' option to upgrade the age	nt which is outside the domain.						
Deploy WinSCP								
Install default Remed	ial Action EXEs on this system 🛈	)						
EventTracker : NTPLDTBLR14								
		Select 'Upgrade' to proceed.						
			Cancel	Back	Next	Advanced	Upgrade	~

Figure 37

6. Check Install default Remedial Action EXEs on this system option to install remedial action scripts.

EventTracker opens a message box.





**Remedial Actions** are scripts or executable files that can be launched at either the agent or the manager side, in response to events. If this option is enabled, predefined scripts will be placed in the



EventTracker\Agent\Script folder at the manager side. These may be installed at the agent side also, during deployment via the **System** manager.

7. Click **OK** to install remedial action EXEs

(OR)

Click Cancel to not to install remedial action EXEs.

The agent will be installed on the selected machine with the default etaconfig.ini configuration.

8. Click Advanced to set a more specific configuration while agent upgrade.

Upgrade Remote agent(s)		×						
Apply configuration After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify the file.								
You can also select 'Default' and configure later.         Image: Configure Con								
Select 'Upgrade' to proceed.								
	Cancel Back Next Advanced Upgrade	:						

Figure 39

The **Default** option is selected by default to apply the manager side 'Agent configuration' settings (etaconfig.ini).

(OR)

Select the **Custom config** option to select a custom configuration file.



The custom configuration will provide the templates you have created in Agent configuration and two more predefined templates.

You can select the template of your choice.

etaconfig\_Servers.ini: This predefined template contains the ideal server configurations which can be applied to the selected agent system.

etaconfig\_Workstations.ini: This predefined template contains the ideal workstation configurations which can be applied to the selected agent system. This option disables the 'Offline event sending' option.

#### 9. Click Upgrade.

EventTracker opens an information message.



Figure 40

10. Click **OK**.

EventTracker opens the System Status screen.



Request Status								×
Application All	✓ Status	All 🗸	Sort by Date	~				
Purge all status older 11/25/2017	than						C 1 Purge	
Date Nov 25 04:50 PM	Group/System	By	Agent EventTracker	<b>Type</b> Upgrade agent	Status New	Description In progress.		
[편] (Ctrl) >							Clo	se

Figure 41

11. Click the  $^{m C}$  button, to see the latest status.

Request Status						
Application All	✓ Status	All V	Sort by Date	~		
Purge all status ol 11/25/2017	der than					C 1 Purge
Date	Group/System	Ву	Agent	Туре	Status	Description
Nov 25 04:53 PM	NTPLDTBLR17	sunanda	EventTracker	Upgrade agent	New	In progress.
Nov 25 04:51 PM	R1S3VM1	Sananad	EventTracker	Upgrade agent	New	In progress.
Nov 25 04:50 PM	NTPLDTBLR14	sunanda	EventTracker	Upgrade agent	Success	Upgrade over ip done successfully.
						Close

Figure 42

**NOTE:** It may take some time to load the status.

**Step 9: Import Knowledge Objects after the upgrade.** (This applies to the customers who have upgraded from v9.0 / v9.1 to v9.3)

Import the latest knowledge objects (KO) after the upgrade. The newly optimized knowledge objects contain improvements in RegEx matching and source type mapping. Refer to the User Guide and knowledge pack portal for more information on knowledge objects.

Note:

- Import EventTracker and Windows KOs on top of existing KO.
- Delete any other KOs and import the new KOs as per the need.
- If new KOs are not imported, only standard properties will be indexed.
- 1. Logon to EventTracker.
- 2. To import Knowledge Objects, select the Admin menu, and then select Knowledge Objects.
- 3. Click Import **T**.
  - EventTracker Knowledge Objects Import/Export window opens.
- 4. Click **Browse** and then select the file from the desired location.

**NOTE:** The file extension should be '.etko' only. The knowledge objects are segmented into folders. Based on the devices the user(s) is using, they can import them which is available in ...\<u>InstallDIR\EventTracker\Knowledge Packs</u>



Choose File to Upload						
🛞 🏵 🔻 🕇 퉬 « EventTr	acker → Knowledge Packs → → ✓ (	Search Knowledg	je Packs 🔎			
Organize 🔻 New folder 🛛 📰 👻 🔟 🍘						
🛛 🏭 Intel 🔷 Na	ame	Date modified	Туре ^			
IPPairGenerato	Accellion Secure File Transfer	11/23/2017 4:21 PM	File folder			
Juniper-test	Aerohive Wireless Access Point	11/23/2017 4:21 PM	File folder			
Logs	Apache Web Server	11/23/2017 4:21 PM	File folder			
Notepad++Por	Barracuda Message Archiver	11/23/2017 4:21 PM	File folder			
PeriLogs	Barracuda Spam Firewall	11/23/2017 4:21 PM	File folder			
Program Files	Barracuda SSL VPN	11/23/2017 4:21 PM	File folder			
Program Files (	Barracuda Web Security Gateway	11/23/2017 4:21 PM	File folder			
Python27	Bluecoat Proxy SG	11/23/2017 4:21 PM	File folder			
Transfording	Check Point Firewall	11/23/2017 4:21 PM	File folder			
	Cisco ACS	11/23/2017 4:21 PM	File folder			
Users	Cisco ASA Firewall	11/23/2017 4:21 PM	File folder			
VirusShare	Cisco IOS	11/23/2017 4:21 PM	File folder 🛛 👻			
Windows V <			>			
File name:		✓ Custom Files (*.	etko) 🗸 🗸			
		Open	Cancel:			

Figure 43

- 5. Click **Open**.
- 6. Click Upload.
- 7. To upload knowledge objects, select the **Object name** option.



Figure 44



#### 8. Click Import.

#### NOTE:

- After upgrading from v9.0/v9.1/v9.2 to v9.3, the user will first have to import the new Token templates (with the extension .ettd) from the install DIR\Program Files\Prism MicroSystems\EventTracker\Configuration Files and then import the newly available Defined Reports (with the extension .issch) from the same path.
- While importing the newly added defined reports from the **EventTracker Control Panel**, the user has to select the Old Type option with extension .issch.

## 3.2 Configuring Service Accounts

If the user is setting UNC path (Uniform Naming Convention) for storing Archives/Reports, then service account of EventTracker Scheduler, EventTracker EventVault, EventTracker Reporter, EventTracker Indexer, and Event Correlator (if available) services should be made to run on the user account having full permission on the set UNC path.

1. Open the "EventTracker Configuration" from Start, and "Run as administrator".



#### Figure 45

2. Configure the same with a user who has full permissions to access the shared archives folder.



🍟 EventTracker :: Configuration	×
Netsurion EventTracker*	
User Credentials	User Authentication
User Name TOONS\Karen	<ul> <li>Local Account</li> </ul>
Password	• Active Directory
EventTracker Group EventTracker	Database Authentication
<i>Note:</i> For "Active Directory" authentication enter user name and pa domain user and for "Local Account" authentication enter loca name and password. User must be administrator on this syste	OK Cancel ssword of a al system user em. Refer <u>install quide</u> .

Figure 46

**\*\*** "Karen" has full permissions to access the archives UNC path.

**NOTE:** You may ignore the above steps, if it is already configured with the required user.

- 1. Click Start, and then select Run.
- 2. Type services.msc and click OK.

Run	? 🗙
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	services.msc
	OK Cancel Browse

Figure 47

3. In the Services window, search for EventTracker services.

File Action: View Help							
◆◆ ● ■ 目 2 () ● ■ = ● = = ●							
C. Services (Local)							
of secures (county)	Services (Local)		_	_	_		
	Mygen-W Heartbeat Service	Norme	Description	Shiftun	Stattup Type	Log On As	
	B 14 1	C Distributed Transaction Coordinator	Coordinates		Manual	Nietovarik S	
	The service	Conto Client	The DNS Cli	Running	Automatic (T	Nietovarik S	
		C Electricoearch 5.5.2 (identicoearch-sen/i	Electionary	Running	Automatic	Local Syste	
	Description	C Encrypting File System (EFS)	Provides th		Manual (Trig	Local Syste	
	Monitors the state of this virtual	🍓 EventTracker Agent	Relays local	Running	Automatic	Local Syste	
	machine by reporting a heartheat at	🔍 EventTracker Alerter	Used by Eve	Running	Automatic	Local Syste	
	you identify running without machines	🍓 EventTracker Elasticsearch Indexer	EventTracke	Running	Automatic	Local Syste	
	that have shopped responding.	🎑 EventTracker EventVault	An EventTra	Running	Automatic	Local Syste	
		🔍 EventTracker Indexer	EventTracke	Running	Automatic	Local Syste	
		🔍 EventTracker Monitoring Daemon	Monitoring	Running	Automatic	Local Syste	
		🔍 EventTracker Receiver	Enables Eve	Running	Automatic	Local Syste	
		🌼 EventTracker Remoting	Agent instal	Running	Automatic	.\EventTra	
		鵒 EventTracker Reporter	Manage rep	Running	Automatic	Local Syste	
		🍓 EventTracker Scheduler	Used by Eve	Running	Automatic	Local Syste	
		🍓 EventTracker WatchList	An EventTra	Running	Automatic	Local Syste	
		C.Edenible Authentication Protocol	The Edensi		BRATSLAN	Local Syste	
		C Family Safety	This service		Manual	Local Service	
		Q, fax	Enablies you		Manual	Nikelburgerfik S	
		C. File Hidtory Service	Protects use		Manual (Trig	Local Syde	
		G Function Discovery Provider Heat	The FORMO		Manual	Local Service	
		Function Discovery Resource Publicati	Publishes th		Manual	Local Service	
		Google Update Service (gupdate)	Kanps your		Automatic (D	Local Syde	
		😘 Google Sydate Service ((pupdaterri)	Kanpo your		Manual	Local Sydie	

#### Figure 48

- 4. Right-click the service name and click **Properties**.
  - For example, Right click EventTracker EventVault service.
  - 'EventTracker EventVault Properties (Local Computer)' dialog box will appear on the screen.

EventTracker EventVa	ult Properties (Local Computer) 🛛 김 🔀				
General Log On Reco	very Dependencies				
Log on as:					
● Local System accour Allow service to in	iteract with desktop				
○ <u>I</u> his account:	Browse				
Password:					
<u>C</u> onfirm password:					
You can enable or disab	le this service for the hardware profiles listed below:				
Hardware Profile	Enabled				
	<u>Enable</u> <u>D</u> isable				
OK Cancel Apply					

Figure 49

5. Click Log On and select This account option.

Log on as:	domain name\ use	r name
O Local System accou	ant	
Allow service to	interact with desktop	_
This account:	toons\karen 🧖	Browse
Password:	•••••	
Confirm password:	•••••	



- Enter the user credentials and correct password.
   The user name should be in the 'domain name\user name' format.
- 7. Click Apply.

A warning message appears.

Services	
⚠	The new logon name will not take effect until you stop and restart the service.
	ОК



- 8. Click **OK**.
- 9. To run the service with the new logon name, stop and start the service.
- 10. Likewise, for the rest of the services, repeat **step 4** to **step 10** to change the service account. The **Log On As** column will display the changed service account name.

Name 7	Description	Status	Startup Type	Log On As
Event Log	Enables ev	Started	Automatic	Local System
EventTracker Agent	Relays loca	Started	Automatic	Local System
EventTracker Alerter	Used by Ev		Automatic	Local System
EventTracker EventVault	An EventTr	Started	Automatic	toons' karen
EventTracker Indexer	EventTrack	Started	Automatic	toons' karen
EventTracker Receiver	Enables Ev	Started	Automatic	Local System
EventTracker Remoting	Agent inst	Started	Automatic	toons\karen
EventTracker Reporter	Manage re	Started	Automatic	toons\karen
EventTracker Scheduler	Used by Ev	Started	Automatic	Toons\ karen
Extensible Authentication Protocol Service	Provides wi		Manual	Local System

Figure 52

Netsurion. EventTracker

# 4. Source Type Mapping

- 1. After appling the update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1), user has to navigate to the following install path "**Prism Microsystems\EventTracker\AdvancedReports**".
- 2. Right click on the "EventTracker.Update.SourceTypeMapping.exe" file and choose "Run as Administrator".
- 3. The Source Type Mapping window appears, click on the "Scan indexed data for syslog sources" button

🔛 Source type mapping		_	$\times$
	Scan indexed data for syslog sources		



The following message appears and click **ok**.
 This message confirms that the source type temp database is created successfully



Figure 54

- 5. Open EventTracker Database.
- 6. Find and edit the **dbo.TempSourceTypeMapping** table and confirm if all the data is avaliable.



If you encounter any problems during the upgrade process, please contact the support team to get quick and thorough instructions.

**Technical Support Contact Details:** Toll-Free: 877-333-1433 ext. 2 Phone: +1-410-953-6776 ext. 2 Fax: +1-410-953-6780 Email: <u>support@eventtracker.com</u>



