

EventTracker Log Management (ETLM): Virtual Appliance Quick Start Guide Version 9.3 Build 5

Publication Date: March 24, 2020

Abstract

The EventTracker Virtual Appliance allows you to capture and manage log data from all types of sources in your enterprise. It installs within minutes and can begin deploying agents, collecting logs, and analyzing data from the configured log sources immediately. This guide assists in setting up the EventTracker Virtual Appliance in your VMware environment.

Scope

The configurations detailed in this guide are consistent with **EventTracker Log Management Version 9.3 Build 5** and **VMware ESX 5.5** or later.

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. Ever	ntTracker Virtual Appliance in VM Ware Environment	3
1.1	Minimum Hardware Requirements	3
1.2	EventTracker Virtual Appliance Details	3
1.3	Prerequisites	4
1.3.	1 Summary	4
1.4	Setting up EventTracker Virtual Appliance	6
1.4.	1 Installing EventTracker Virtual Appliance	6
1.4.2	2 Importing EventTracker Virtual Appliance	6
1.5	Upgrading Virtual Hardware	11
1.6	Adding a new Network adapter	12
1.6.3	1 Removing an existing network interface	12
1.6.2	2 Adding a new network interface	15
1.7	Configuring EventTracker Virtual Appliance	



1. EventTracker Virtual Appliance in VM Ware Environment

1.1 Minimum Hardware Requirements

The minimum VM requirement to import EventTracker virtual appliance on VMware ESX/Esxi.

- CPU 8 Core @2.5 GHz minimum
- Memory 16 GB
- VM Controller LSI Logic RAID
- VM Hard Drive SCSI/SSD type
- Disk 300 GB
- Network Adapter 1

1.2 EventTracker Virtual Appliance Details

- EventTracker OVF file size 13 GB
- Hostname ETConsole
- WorkGroup EventTracker
- Disk Space: 300 GB (33 GB initial)
- CPU 8 Core @2.5 GHz minimum
- **Memory** 16 GB
- VM Hard Drive SCSI/SSD type
- IP Address Assign Static IP address
- Operating System Windows server 2019 Standard Edition
- Web Server IIS 11
- Database Server Microsoft SQL Server 2017 Express Edition
- EventTracker Version 9.3 Build 5 ETLM

1.3 Prerequisites

- EventTracker customer must have a license key for Microsoft Windows 2019 Standard edition.
- The 30-days grace period is not available In Microsoft Windows Server 2019. If the operating system is
 not activated, watermark appears showing the Windows edition (although it does not show to
 activate) On the desktop, personalization features in PC Settings like changing the lock screen is
 disabled. Entire screen notification appears periodically. However, the operating system continues to
 function normally.
- User must provide a product key and activate.

1.3.1 Summary

- 1. Download the .ova file from the link provided by the EventTracker technical support.
- 2. Get the EventTracker license from the EventTracker technical support.
- 3. Import OVF to VMware ESX.
- 4. Install VMware guest tools on the newly imported VM.
- 5. Login as ETAdmin,
 - Change the Computer name, connect it to the domain if the active directory authentication is required, else leave it as it is for local account authentication and restart the Virtual Machine.
 - Run the downloaded batch file UpdateSystemName.bat in the command prompt available in the C:\UpdateSystemName\directory.

-> • 🛧 📙	> Thi	s PC > Local Disk (C:) > UpdateSystem	NameV9_3_ETLM				~ Ū	Search UpdateSystemName	ρ
		Name	Date modified	Туре	Size				
Quick access	*	UpdateESPath.vbs	1/17/2020 9:00 AM	VBScript Script File	1	KB			
		UpdateSystemName.bat	1/17/2020 9:00 AM	Windows Batch File	1	KB			
Downloads	*	😰 UpdateSystemName.vbs	2/22/2019 11:38 AM	VBScript Script File	4	KB			
Documents	*								
Pictures	A								
Agent									
RemoteInstalle									
UpdateSystem	Nam								
This PC									
Network									

Figure 1

- 6. Update the credentials in the EventTracker.
- 7. Change **startup** to **Automatic** for following EventTracker Services and start the service.
 - EventTracker Agent
 - EventTracker Alerter
 - EventTracker EventVault
 - EventTracker Indexer
 - EventTracker Receiver
 - EventTracker Remoting
 - EventTracker Reporter
 - EventTracker Scheduler
 - Elasticsearch 7.2.1 (elasticsearch-service-x64)
 - EventTracker Elasticsearch Indexer
 - EventTracker Monitoring Daemon
- 8. Install EventTracker license using EventTracker License Management.
- 9. Run Microsoft Windows updates to install the latest windows updates and security patches.
- 10. Install the latest EventTracker updates.
- 11. Start EventTracker Evaluation.

NOTE:

- Microsoft Windows OS will continue to run the 30 days trial without activation. To continue using you need to activate Microsoft Windows using a valid license key.
- No antivirus software is installed by default. It is recommended to install antivirus software.



1.4 Setting up EventTracker Virtual Appliance

1.4.1 Installing EventTracker Virtual Appliance

- 1. Ensure that you are using fully functional VMware ESX/ESXi 5.5 or later.
- 2. Get EventTracker Evaluation license from the EventTracker support.
- 3. Download the '.ova' file from the link provided by the EventTracker technical support.
- 4. Follow the instructions provided in a detailed section (Import EventTracker virtual appliance) to import the downloaded OVA file.

1.4.2 Importing EventTracker Virtual Appliance

- 1. Login to the VMWare VCenter console and select the host.
- 2. In the vSphere Web Client, click the File menu, and select Deploy OVF Template.

vmware [®] vSphere W	/eb Client ≜ ≣										
Navigator	Ŧ	172.30.1.47	8 2 D I	🗈 📘 🚳 Acti	ons 👻						
A Back		Getting Started	Summary Moni	tor Configure	Permissi	ions VMs	Resource Pools	Datastores	Networks	Update Ma	nager
▶ 🗍 172 3 Ne	Q ions - 172.30.1.47 w Virtual Machine w VApp		Hypervisor: Model: Processor Typ Logical Proces NRCa: Virtual Machine State: Uptime:	sors: 24 2		331820 5660 @ 2.80G	Hz				
▶ 🔂 172 3 🏷 Ne	w Resource Pool ploy OVF Template	 Hardware 				Config	uration				
ETV/AD		▶ • Tags				 Custor 	m Attributes				
Et EventT		Assigned Tag	Category	Description		Attribute	Value				
🔂 R1P1S			This list is em	pty.	_	AutoDeplo	y.Ma				
M RIPIS		-									
Ph Sharan	-	•									
	Id Networking Id Diagnostic Partition										
ETVAS Ho	st Profiles	•		Assign F	Remove				F	dit	
🖧 V9esse Ed	it Default VM Compatibility	_		, original i	<u></u>						
y9etime Ex	port System Logs	 Related O 	bjects			-	e Manager Compl	iance			
▶ 1725 Re	configure for vSphere HA				.111	Status	② Unknown				
	sign License										
Se	ttings										
	ove To										
Task Name Tag	gs & Custom Attributes	tatus		Initiator	0	Queued For	Start Time	1 🔻	Completion Ti	me	Server
Ad	ld Permission										
		•									
	emove from Inventory sassociate Host										
	vCenter Orchestrator plugin Actions date Manager										

Figure 2



3. In the **Deploy OVF Template** wizard, browse and select the downloaded file, and then select **Next >**.

🎁 Deploy OVF Template		? ₩
1 Select template 2 Select name and location	Select template Select an OVF template.	
 2 Select name and location 3 Select a resource 4 Review details 5 Select storage 6 Ready to complete 	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
	Back Next Finish Can	cel

Figure 3

4. Select the name and location and click **Next≥.**

8	Deploy OVF Template		(? H
~	Select template Select name and location	Select name and location Enter a name for the OVF and select a deployment location.	
	3 Select a resource	Name EventTracker_9_3_B5_ETLM	
	4 Review details	Filter Browse	
	5 Select storage 6 Ready to complete	Select a datacenter (0) or (1) folder.	
		Back Next Fini	ish Cancel

Figure 4



5. Select the host where you want to run the deployment and click Next \geq .

Deploy OVF Template		- ? >
 1 Select template 2 Select name and location 	Select a resource Select where to run the deployed template.	
 3 Select a resource 4 Review details 5 Select storage 6 Ready to complete 	Filter Browse Select a host {0} or {1} cluster {0} or {1} resource pool {0} or {1} vapp. ITTE:00:1:020 ITTE:00:1:021 ITTE:00:1:024 ITTE:00:1:023 ITTE:00:1:07 (not responding) ITTE:00:1:07 ITTE:00:1:07 ITTE:00:1:07 ITTE:00:1:07 ITTE:00:1:07 ITTE:00:1:07 ITTE:00:1:07 ITTE:00:1:07 ITTE:00:1:03 ITTE:00:1:04 ITTE:00:1:04 ITTE:00:1:05 ITTE:00:1:05 ITTE:00:1:05 ITTE:00:1:05 ITTE:00:1:05 ITTE:00:1:05 ITTE:00:1:05 <liitte:00:1:05< li=""></liitte:00:1:05<>	
	Back Next Finish	Cancel

Figure 5

6. **Review the details** and click **Next** ≥.

X	Deploy OVF Template			• •
	1 Select template 2 Select name and location	Review details Verify the template	e details.	
	 3 Select a resource 4 Review details 5 Select storage 6 Select networks 7 Ready to complete 	Publisher Download size Size on disk	 No certificate present 13 GB 31.9 GB (thin provisioned) 300.0 GB (thick provisioned) 	
			Back Next Fir	nish Cancel

Figure 6

7. To store the virtual disks, select the disk format as **Thin Provision format**, and click **Next** ≥.



🍘 Deploy OVF Template					(?) ₩
 1 Select template 2 Select name and location 3 Select a resource 4 Review details 5 Select storage 	Select storage Select location to store the files for the Select virtual disk format: Thin pro	vision	•		
6 Select networks 7 Ready to complete	Filter Datastores Datastore Clusters]	(🖲 🃡 📑 Q Filte	· •
	Name Name Additional of the second	Status Warning	VM storage policy	Capacity 2.72 TB	Free 427.42 GB
			Bac	k Next	Finish Cancel

Figure 7

8. Select a destination network for each source network and click Next ≥.

🏷 Deploy OVF Template		?	**
 1 Select template 2 Select name and location 	Select networks Select a destination network for each source network.		_
✓ 3 Select a resource	Source Network	Destination Network	
✓ 4 Review details	VM Network	VM Network 🔹	
✓ 5 Select storage			
6 Select networks			
7 Ready to complete			
			_
	IP Allocation Settings		
	IP protocol: IPv4	IP allocation: Static - Manual 🚯	
		Back Next Finish Cancel]_

Figure 8



9. Review the deployment settings and click **Finish**.

Peploy OVF Template				? »
 1 Select template 2 Select name and location 	Ready to complete Review configuration data.			
✓ 3 Select a resource	Name	EventTracker_9_3_B5_ETLM		
 4 Review details 5 Select storage 	Source VM name	EventTracker_9_3_B5_ETLM		
 ✓ 5 Select storage ✓ 6 Select networks 	Download size	17.6 GB		
 7 Ready to complete 	Size on disk	31.9 GB		
V Ready to complete	Datacenter	DO Outentile		
	Storage mapping	1 7		
	Network mapping	1		
	IP allocation settings	IPv4, Static - Manual		
	, in choose of the second			
			Back Next Finish	Cancel
				.1

Figure 9

10. The progress bar of the import task appears on the screen.

🛐 Recent Tasks							
• -							
Task Name	Target	Status	Initiator	Queued For	Start Time 1	Completion Time	Server
Deploy OVF template	EventTracker_9_3	40 % 🛞	VSPHERE.LOCAL\\	4 ms	2/22/2019 4:39:41 AM		vcenter.prismusa.com
Import OVF package	17. 47	40 % 🛞	PRISMUSA\\nagend	105 ms	2/22/2019 4:31:23 AM		vcenter.prismusa.com

Figure 10

11. Once the deployment is completed, it displays the status as "**Completed**".

😴 Recent Tasks		
₽ -		
Task Name	Target	Status
Deploy OVF template	EventTracker_9_3	 Completed
Import OVF package	17: 17	 Completed





1.5 Upgrading Virtual Hardware

If the OVA is imported on ESX5.5 using VSphere client to manage host, editing the Virtual Machine should be done before upgrading the Hardware.

1. Right-click on the imported Virtual Machine and select Upgrade Virtual Hardware.

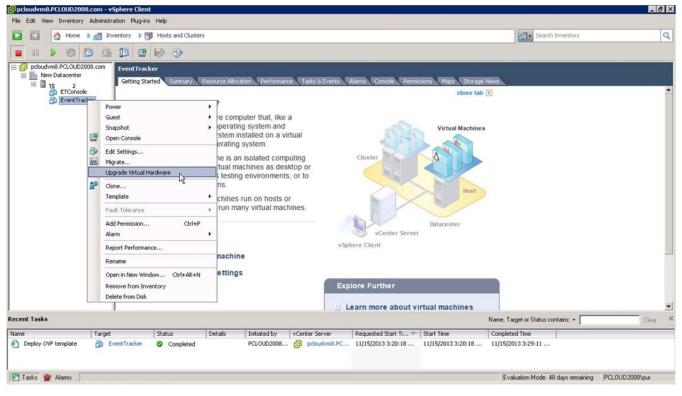


Figure 12

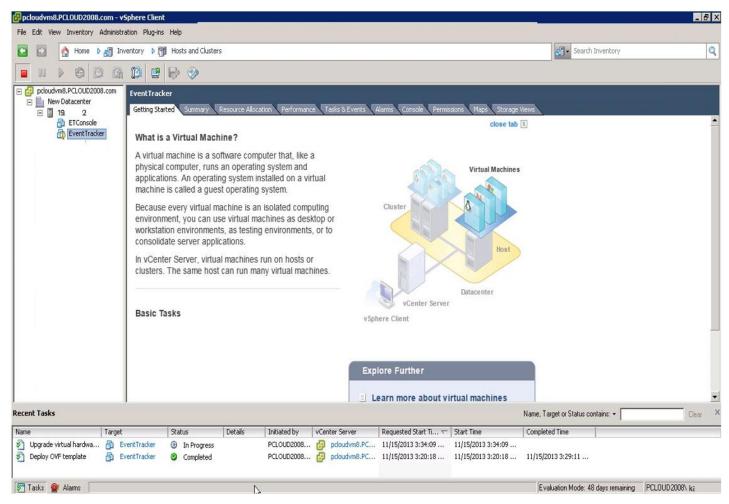
2. A warning message displays to Confirm the Virtual Machine Upgrade.



Figure 13



3. Click Yes. In Recent Tasks pane, a message displays stating that the upgrade is in 'In Progress' status.





1.6 Adding a new Network adapter

The network adapter provides backward compatibility. After deploying OVA, the user can edit VMware and remove the existing network interface. Later a new network interface is added by selecting the Interface type VMXNET 2 (Enhanced) or VMXNET 3 depending on VMware ESX version.

1.6.1 Removing an existing network interface

1. To remove an existing network interface, right-click on the machine and select Edit Settings...



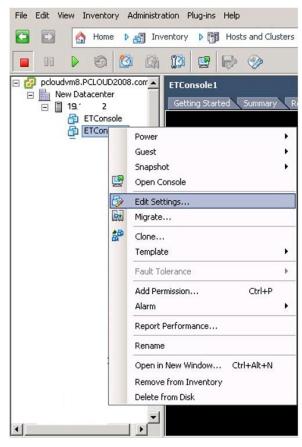


Figure 15

2. Virtual Machine Properties window opens.

Show All Devices	Add Remove	Device Status
ardware	Summary	Connect at power on
Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD Drive 1	16384 MB 8 Video card LSI Logic Parallel Virtual Disk CD/DVD Drive 1	Adapter Type
Network adapter 1	VM Network	Automatic Manual
VMCI device	Restricted	Network Connection Network label:
		VM Network





3. Click **Remove** and then click **OK**.

the removal, click the Restore button.

Figure 17

Note: The memory and the CPU need to be set according to our standard that is mentioned in the page number 3.

ETConsole1 - Virtual Machi Aardware Options Resources		Virtual Machine Version: 7
Show All Devices	Add Remove	Device Status
Hardware Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD Drive 1 Network adapter 1	Summary 16384 MB 8 Video card LSI Logic Parallel Virtual Disk CD/DVD Drive 1 VM Network	Connect at power on Adapter Type Current adapter: E1000 MAC Address 00:50: 10:03 C at terretion C Macual
WMCI device	Restricted	Automatic C Manual Network Connection Network label: VM Network
Help		OK Cancel

Figure 18



1.6.2 Adding a new network interface

To add an enhanced network adapter,

1. Right-click any machine and select Edit Settings....

Virtual Machine Properties window opens.

ETConsole1 - Virtual Machin	Virtual Machine Version: 7
Hardware Options Resources Show All Devices Hardware Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD Drive 1 VMCI device	Virtual Machine Version: 7 Virtual Machine Version: 7 Memory Configuration US55 GB Memory Size: B GB G
Help	 OK Cancel

Figure 19

2. Select Add....

Add Hardware window opens.



Device Type Ready to Complete	Choose the type of device you v	vish to add.
	 Serial Port Parallel Port Floppy Drive CD/DVD Drive USB Controller USB Device (unavailable) PCI Device (unavailable) Ethernet Adapter Hard Disk SCSI Device 	- Information

Figure 20

3. Select the Device Type, and then click Next >.

evice Type etwork connection eady to Complete	Adapter Type Type: VMXNET 3 E1000 Adapter ch VMXNET 2 (Enhanced) Consult the VMXNET 3 pr more information on choosing among the network adapters supported for various guest operating systems and hosts.
	Network Connection Named network with specified label: VM Network Legacy network: Legacy network: Legacy network types are not fully compatible with migration between hosts.
	Device Status Connect at power on

Figure 21



- 4. In Adapter Type pane, select Type: drop-down, and then select VMXNET 2 (Enhanced) or VMXNET 3.
- 5. Click Next >.
 - Ready to Complete page opens.

Review the selected opt	tions and click Finish to add th	ne hardware.		
Device Type Network connection	Options:			
Ready to Complete	Hardware type: Adapter type: Network Connection: Connect at power on:		 	

Figure 22

6. Click Finish.

A successful message opens.

ardware Options Resources		Virtual Machine Version: 1
Show All Devices	Add Remove	Device Status
lardware	Summary	Connect at power on
Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD Drive 1 VMCI device New NIC (adding)	16384 MB 8 Video card LSI Logic Parallel Virtual Disk CD/DVD Drive 1 Restricted VM Network	Adapter Type Current adapter: VMXNET 2 (Enhanced) MAC Address Automatic C Manual Network Connection Network label:
Help		VM Network

Figure 23



1.7 Configuring EventTracker Virtual Appliance

Once EventTracker Virtual appliance is deployed successfully, make few configuration changes as below:

- 1. Power on the EventTracker Virtual machine.
- 2. Log in to 'EventTracker Virtual' system as EventTracker administrator using below credential.
 - Username: ETConsole\ETAdmin
 - Password: Welc0me@129#

NOTE: On the first successful logon you will be prompted to change the ETAdmin user password. Change it to secure password and keep it safe.

- 3. Change Computer name, join it to domain if active directory authentication is required else leave it as it is for local account authentication and restart the Virtual Machine.
- 4. Download the zip file from the below link:

https://downloads.eventtracker.com/downloads/utils/UpdateSystemNameV9 3 ETLM.zip

and then copy on a local drive and extract this file in C:\UpdateSystemName\directory.

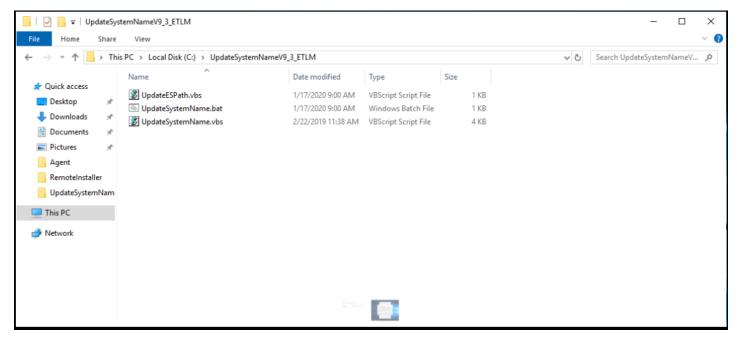


Figure 24

5. After extracting , run the UpdateSystemName.bat file.

6. Navigate to C:\Program Files (x86)\Prism Microsystems\EventTrackerWeb\bin folder and run the executable file evtInstallConfig.exe.

EventTracker :: Configuration	×
Netsurion EventTracker*	
User Credentials	User Authentication
User Name ETAdmin	Local Account
Password	Active Directory
EventTracker Group EventTracker	Database Authentication
Note:	OK Cancel
For "Active Directory" authentication enter user name a domain user and for "Local Account" authentication enter name and password. User must be administrator on this	er local system user



- 7. Update the user credential ETAdmin user or select an active directory and enter domain user credentials.
- 8. Once **EventTracker Configuration** validates the credential and runs successfully, install **VMware Tools** on newly imported Virtual machine.
- 9. Change startup type to Automatic for following EventTracker Services and start the service.
 - EventTracker Agent
 - EventTracker Alerter
 - EventTracker Elasticsearch Indexer
 - EventTracker EventVault
 - EventTracker Indexer
 - EventTracker Monitoring Daemon

- EventTracker Receiver
- EventTracker Remoting
- EventTracker Reporter
- EventTracker Scheduler
- Elasticsearch 7.2.1 (elasticsearch-service-x64)
- EventTracker Elasticsearch Indexer
- EventTracker Monitoring Daemon
- 10. Navigate to C:\Program Files (x86)\Prism Microsystems\EventTracker\ folder, and execute the file ETControlPanel.exe.

EventTracker Control Panel window opens.



Figure 26

11. Double click on the License Manager and verify the license.



🗐 EventTrack	er - License Manager	\times
Evaluation	EventTracker Security LLC Product : EventTracker Version : 9.0 Account Id : 99999-9999 Edition : ETLM	
Issued To: Issued By: Date Installed:	EventTracker Log Manager Evaluation 9_3,99999-9999,EventTracker Log Manager EventTrackerCA,EventTracker Security LLC,Columbia,US 23-MAR-2020 Support Expires on: 13-APR-2020 License Expires on: 13-APR-2020	
Status: Upgrade Li	View Certificate View Features View Usage Save Details	^ ~

Figure 27

After successful installation, login to **EventTracker Web** using ETConsole\ETAdmin user credentials in the web browser.

NOTE:

Log in to 'EventTracker' Virtual Machine as ETConsole\administrator and change the system password for future reference. Secure the system using a strong password.



General	
Guest OS:	Microsoft Windows Server 2019 (64-bit)
VM Version:	8
CPU:	4 vCPU
Memory:	6144 MB
Memory Overhead:	340.39 MB
VMware Tools:	Running (Current)
IP Addresses:	1 5 View al
DNS Name:	pcloud37-vm7.PCLOUD2008.com
State:	Powered On
Host:	pcloud37.prismusa.com
Active Tasks:	
vSphere HA Protection:	③ N/A 🖓

Figure 28

