

Quick Start Guide

EventTracker Security Center: VMWare Virtual Appliance

Version 9.3.13

Publication Date:

August 18, 2022

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.

Audience

This guide is intended for use by all EventTracker users responsible for investigating and managing network security. This guide assumes that you have EventTracker access and an understanding of networking technologies.



Table of Contents

1 Event	tTracker Virtual Appliance in VMWare Environment	.4
1.1 N	/inimum Hardware Requirements	.4
1.2 E	eventTracker Virtual Appliance Details	.4
1.3 P	Prerequisites	.5
1.3.1	Summary	.5
1.4 S	Setting up EventTracker Virtual Appliance	.6
1.4.1	Installing EventTracker Virtual Appliance	.6
1.4.2	Importing EventTracker Virtual Appliance	.7
1.5 U	Jpgrading Virtual Hardware	12
1.6 A	Adding a new Network adapter	13
1.6.1	Removing an existing Network Interface	14
1.6.2	Adding a new Network Interface	15
1.7 C	Configuring EventTracker Virtual Appliance	19

Netsurion

1 EventTracker Virtual Appliance in VMWare 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 12.6 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 ETSC Collection Point
- EventTracker Updates Applied ET93U20-2005, ET93U20-008, ET93U20-8009, ET93U21-043, ET93U21-044, ET93U21-046, ET93U21-047, ET93U21-048, ET93U21-049, ET93U21-050, ET93U21-051, ET93U21-052, ET93U21-053, ET93U21-054, ET93U21-055, ET93U21-056, ET93U21-057, ET93U21-058, ET93U21-059, ET93U21-060, ET93U21-8010, ET93U21-062, ET93U22-063, ET93U22-064, ET93U22-8011, ET93U22-066, ET93U22-067, ET93U22-068, ET93U22-8012, ET93U22-069, ET93U22-070.



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. Log in 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.



- 6. Update the credentials in the EventTracker.
- 7. Change startup to Automatic for following EventTracker Services and start the following services.
 - EventTracker Agent
 - EventTracker Alerter
 - EventTracker EventVault

Netsurion

- EventTracker Indexer
- EventTracker Receiver
- EventTracker Remoting
- EventTracker Reporter
- EventTracker Scheduler
- Elasticsearch 7.2.1 (elasticsearch-service-x64)
- EventTracker Elasticsearch Indexer
- EventTracker Monitoring Daemon
- WCW Service
- Traptracker Receiver
- 8. Install EventTracker license using **EventTracker License Manager**.
- 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 to use 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. Log in to the VMWare VCenter console and select the host.
- 2. In the vSphere Web Client, click the File menu, and select Deploy OVF Template.



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



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

Participate Control		(?)÷
 1 Select template 2 Select name and location 	Select name and location Enter a name for the OVF and select a deployment location.	
 3 Select a resource 4 Review details 5 Select storage 6 Ready to complete 	Name EventTracker_9_3B5_ETSC Filter Browse Select a datacenter (0) or (1) folder.	
	Back Next	Finish Cancel

Netsurion®

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. 110.000.000 110.000.000 110.000.000 110.000.000 110.000.000 110.000.000 110.000.000 110.000.000 110.000.000 110.000.000 110.000.000	*
	Back Next Finish	Cancel

6. Review the details and click Next ≥.

🍘 Deploy OVF Template			(?) ₩
1 Select template2 Select name and location	Review details Verify the template	details.	
✓ 3 Select a resource	Publisher	(2) No certificate present	
4 Review details	Download size	12.6 GB	
5 Select storage 6 Select networks	Size on disk	31.9 GB (thin provisioned) 300.0 GB (thick provisioned)	
7 Ready to complete			
		Back Next Finish	Cancel

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 	Select storage Select location to store the files	for the deployed template.				
 3 Select a resource 	Select virtual disk format: Thi	n provision	•			
✓ 4 Review details	Show datastores from Storage DRS clusters					
5 Select storage 6 Select networks 7 Ready to complete	Filter Datastores Datastore Clus	sters			Filter +	
	Name	Status	VM storage policy	Capacity	Free	
	• 🛃 datastore1 (14)	A Warning	-	2.72 TB	427.42 GB	
	۰ ۸	::			► 1 Objects 🔓 Copy –	
			Bi	ack Next	Finish Cancel	

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 netwo	ĸ.	
✓ 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	

Netsurion®

9. Review the deployment settings and click Finish.

🎲 Deploy OVF Template				? H
 1 Select template 2 Select name and location 	Ready to complete Review configuration data.			
 3 Select a resource 4 Review details 5 Select storage 6 Select networks 7 Ready to complete 	Name Source VM name Download size Size on disk Datacenter Resource	EventTracker_9_3_B5_ETSC EventTracker_9_3_B5_ETSC 12.6 GB 31.9 GB D0 Oxfamble 1 7		
	 Storage mapping Network mapping IP allocation settings 	1 1 IPv4, Static - Manual		
			Back Next Finish	Cancel

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

11. After 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.



A warning message displays to confirm the Virtual Machine Upgrade.

2. Click Yes.



Netsurion®

3. In Recent Tasks pane, a message display stating the upgrade is '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.



2. Virtual Machine Properties window displays.

Show All DevicesAdd	Persoue Device Status
Indune Commany	Connected
Memory Memory	Adapter Type Current adapter: E1000 MAC Address 00:50 00:03
WMCI device Restricted	Automatic Manual Network Connection Network label: VM Network

Netsurion

3. Click Remove and click OK.

Hardy	ware Options Resources		Virtual Machine Version: 7
	Show All Devices	Add Restore	This device has been marked for removal from the virtual machine when the OK button is clicked.
	ware Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD Drive 1 Network adapter 1 (removing) VMCI device	Summary 16384 MB 8 Video card LSI Logic Parallel Virtual Disk CD/DVD Drive 1 Removed Restricted	To cancel the removal, click the Restore button.
	Help		OK Cancel

Note: The memory and the CPU need to be set according to our standard mentioned in the <u>requirements</u> page.

Hardware Summary Memory 16384 MB CPUs 8 Video card Video card SCSI controller 0 LSI Logic Parallel Hard disk 1 Virtual Disk CD/DVD Drive 1 CD/DVD Drive 1 Network adapter 1 VM Network WMCI device Restricted	Show All Devices	Add Remove	Device Status
Memory 16384 MB CPUs 8 Video card Current adapter Type SCSI controller 0 LSI Logic Parallel Hard disk 1 Virtual Disk CD/DVD Drive 1 CD/DVD Drive 1 Network adapter 1 VM Network VMCI device Restricted	rdware	Summary	Connect at power on
ScSI controller 0 LSI Logic Parallel Hard disk 1 Virtual Disk CD/DVD Drive 1 CD/DVD Drive 1 Network adapter 1 VM Network VMCI device Restricted	Memory CPUs Wideo card	16384 MB 8 Video card	Adapter Type Current adapter: E1000
Network adapter 1 VM Network VMCI device Restricted Network Connection Network label:	SCSI controller 0 Hard disk 1 CD/DVD Drive 1	LSI Logic Parallel Virtual Disk CD/DVD Drive 1	MAC Address 00:50: 10:03
VMCI device Restricted Network Connection Network label:	Network adapter 1	VM Network	Automatic C Manual
VM Network	g VMCI device	Restricted	Network Connection Network label:

1.6.2 Adding a new Network Interface

To add an enhanced network adapter,

- 1. Right-click any machine and select Edit Settings.
- 2. Virtual Machine Properties window displays.

dware Options Resources	5	Virtual Machine Version: 7
dware Options Resource: Show All Devices rdware Memory CPUs Video card SCSI controller 0 Hard disk 1 CD/DVD Drive 1 VMCI device	Add Remove	Virtual Machine Version: : Memory Configuration 255 GB Memory Size: 8 G GB 128 GB Maximum recommended for this 4 guest OS: 255 GB. Maximum recommended for best 9 performance: 8188 MB. Default recommended for this 9 guest OS: 4 GB. 16 GB Jellit Recommended for this 9 guest OS: 512 MB. 1 GB Jellit Recommended for this 9 guest OS:
		64 MB - 32 MB - 16 MB - 8 MB - 4 MB -

3. Click Add to go to the Add Hardware window.

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

4. Select the **Device Type** and click **Next** >.

Retwork connection Ready to Complete	Type: VMXNET 3 E1000 Adapter ch/VMXNET 2 (Enhanced) rking performance and migration compatibility.
	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 C Legacy network:
	Legacy network types are not fully compatible with migration between hosts. Device Status

5. In the Adapter Type pane, select Type: drop-down, and select VMXNET 2 (Enhanced) or VMXNET 3.

6. Click Next and the Ready to Complete page opens.

Device Type Network connection	Options:			
Ready to Complete	Hardware type: Adapter type: Network Connection: Connect at power on:	Ethernet Adapter VMXNET 2 (Enhanced) VM Network Yes		

7. Click Finish and a successful message pops-up.

Show All Devices	Add Remove	Device Status
lardware	Summary	Connect at power on
Memory CPUs SCSI controller 0 Hard disk 1 CD/DVD Drive 1 WMCI 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: VMXINET 2 (Enhanced) MAC Address Automatic C Manual Network Connection Network label:
Help		VM Network

1.7 Configuring EventTracker Virtual Appliance

After 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 <u>Update System Name</u> zip file on local drive and extract this file.



5. Run the UpdateSystemName.bat file.

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

EventTracker :: Configuration	×
Netsurion EventTracker*	
User Credentials User Name ETAdmin Password *******	User Authentication
EventTracker Group EventTracker	Database Authentication
Note: For "Active Directory" authentication enter user name a domain user and for "Local Account" authentication ent name and password. User must be administrator on thi	OK Cancel and password of a er local system user s system. Refer <u>install quide</u> .

- 7. Update the user credential ETAdmin user or select an active directory and enter domain user credentials.
- 8. After 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 following services.
 - 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
 - WCW Service
 - Traptracker Receiver
- **10.** Navigate to **D:\Program Files (x86)\Prism Microsystems\EventTracker** folder and execute the file **ETControlPanel.exe**.

Netsurion®

11. The EventTracker Control Panel window displays.



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

🗐 EventTrack	ker - License Manager	\times			
Evaluatio	n EventTracker Security LLC Product : EventTracker Version : 9.0 Account Id : 99999-9999 Edition : Enterprise				
Issued To: Issued By: Date Installed	Issued To: ET93B5R130VA,999999999999999999999999999999999999				
Status: Upgrade L	Status success View Certificate View Features View Usage Save Details .icense Update CRL Internet Connection Close	~			

13. 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:	8 vCPU
Memory:	16 GB
Memory Overhead:	340.39 MB
VMware Tools:	Running (Current)
IP Addresses:	1 5 View all
State:	Powered On
Active Tasks:	
vSphere HA Protection:	② N/A 모

About Netsurion

Netsurion[®] delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at <u>www.netsurion.com</u>.

Contact Us

Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

713-929-0200

https://www.netsurion.com/company/contact-us