EventTracker: Virtual Appliance

Quick Start Guide

Version 7.6
Abstract

The EventTracker Virtual Appliance enables 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 configured log sources immediately. This guide enables you to quickly set up the EventTracker Virtual Appliance in your VMware environment.

Scope

The configurations detailed in this guide are consistent with EventTracker Version 7.6 and VMware ESX 5.5 or later.
# Table of Contents

Abstract .................................................................................................................. 1  
Scope ..................................................................................................................... 1  
EventTracker Virtual Appliance in VM Ware environment ................................... 3  
  Minimum Hardware Requirements ...................................................................... 3  
  EventTracker Virtual Appliance Details ............................................................... 3  
Prerequisites ......................................................................................................... 4  
Summary ................................................................................................................. 5  
Set Up EventTracker Virtual Appliance ............................................................... 7  
  Install EventTracker Virtual Appliance ............................................................... 7  
  Import EventTracker Virtual Appliance ............................................................... 7  
Upgrade Virtual Hardware ...................................................................................... 12  
Add a new Network adapter ................................................................................... 14  
  Remove an existing network interface ............................................................... 14  
  Add a new network interface .............................................................................. 16  
Configure EventTracker Virtual Appliance .......................................................... 20
EventTracker Virtual Appliance in VMware environment

Minimum Hardware Requirements

Following are the minimum VM requirement to Import EventTracker virtual appliance on VMware ESX/Esxi.

- **CPU** – 2.5 GHz minimum
- **Memory** – 4 GB (6 GB Recommended)
- **VM Controller** – LSI Logic RAID
- **VM Hard Drive** – SCSI type
- **Disk** – 160 GB
- **Network Adapter** – 1

EventTracker Virtual Appliance Details

- **EventTracker OVF file size** – 7.65 GB
- **Hostname** – ETConsole
- **WorkGroup** – EventTracker
- **Disk Space**: 160 GB (12.6 GB initial)
- **CPU** – 2.5 GHz minimum
- **Memory** – 4 GB
- **VM Hard Drive** – SCSI type
- **IP Address** – Assigned by DHCP
- **Operating System** – Windows server 2012 R2 Datacenter Edition SP1 Server core with minimal interface
EventTracker: Virtual Appliance

- **Web Server** – IIS 8.5
- **Database Server** – Microsoft SQL Server 2012 Express Edition
- **EventTracker Version** – 7.6 Build 21 Collection Point Edition

**Prerequisites**

- EventTracker user must have license key for Win 2012.
- In Windows 8, Windows 8.1, Windows Server 2012 and Windows Server 2012 R2, the 30-day grace period has been removed. If the operating system is not activated, there is a watermark showing the edition of Windows (although it does not show to activate) on desktop, personalization features in PC Settings like changing the lock screen is disabled. Entire Screen notification appears periodically. However, the operating system otherwise functions normally.

- User may provide a product key and may choose not to activate.

**NOTE:** This is Server core version of OS and windows desktop will not be shown.
Summary

1. Download the .ova file from the link provided by EventTracker Technical Support.
2. Please get the EventTracker license from EventTracker Technical support.
3. Import OVF to VMware ESX.
4. Install VMware Guest tools on newly imported VM.
5. Login as ETAdmin,
   - 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.
   - Run the batch file UpdateSystemName.bat in command prompt available in C:\ drive.

6. Update the credentials in EventTracker.
7. Change start up to Automatic for following EventTracker Services and start the service.
   - EventTracker Agent
   - EventTracker Alerter
   - EventTracker EventVault
   - EventTracker Indexer
   - EventTracker Receiver
   - EventTracker Remoting
   - EventTracker Reporter
8. Install EventTracker license using **EventTracker License Manager**.

9. Run Windows updates to install latest windows updates and security patches.

10. Install Latest EventTracker updates.

11. Start **EventTracker Evaluation**.

**NOTE:**

- Microsoft Windows OS will continue to run 30 days without activation. If you want to continue after that you need to activate windows using valid license key.

- No antivirus software is installed by default. It is recommended to install antivirus software.
Set Up EventTracker Virtual Appliance

Install EventTracker Virtual Appliance

1. Ensure that you are using fully functional VMware ESX/ESXi 5.0 or later.
2. Get EventTracker Evaluation License by requesting to EventTracker Support.
3. Download the '.ova' file from the link provided by EventTracker Technical Support.
4. Follow the instructions provided in detailed section (Import EventTracker Virtual appliance) to import the downloaded OVA file.

Import EventTracker Virtual Appliance

1. Connect to VMware VCentre server using VI Client using appropriate user credentials.
2. In the vSphere Client, click the File menu, and then select Deploy OVF Template.
3. In the **Deploy OVF Template** wizard, browse and select the downloaded file, and then select **Next >**.
4. Verify the **OVF Template Details** page, and then click **Next ≥**.

![Figure 5](image5.png)

**Figure 5**

5. If required, edit the **VMName** and then select the Datacenter within the inventory where the **vApp** resides.

![Figure 6](image6.png)

**Figure 6**

6. Click **Next ≥**.
7. Select the host or cluster on which you wish to deploy the OVF template, and then click **Next ≥**.

Figure 7

8. To store the virtual machine virtual disks, select the disk format as **Thin Provisioned format**, and click **Next ≥**.

Figure 8

9. Review the deployment settings, and then click **Finish**.
The progress bar of the import task appears on the screen.

10. Click the Close button to complete the deployment process.
Upgrade Virtual Hardware

If OVA is deployed on VMware ESX 4 or later version then VM Hardware has to be upgraded.

**NOTE:**

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

1. Right-click on imported Virtual Machine, and then select **Upgrade Virtual Hardware**.

Figure 12

A warning message displays to Confirm Virtual Machine Upgrade.
2. Click the **Yes** button.

In Recent Tasks pane, a message displays stating that the upgrade is in ‘In Progress’ status.
Add a new Network adapter

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

Remove an existing network interface

1. To remove an existing network interface, right-click the machine and select Edit Settings...
Virtual Machine Properties window displays.

![Virtual Machine Properties Window](image)

**Figure 16**

2. Click **Remove** and then click the **OK** button.
Add a new network interface

To add an enhanced network adapter,

1. Right-click any machine and then select **Edit Settings**...  
   Virtual Machine Properties window displays.
2. Select the Add... button.

Add Hardware window displays.
3. Select the **Device Type**, and then select the **Next >** button.
4. In **Adapter Type** pane, select **Type**: drop-down, and then select **VMXNET 2 (Enhanced)** or **VMXNET 3**.

5. Select the **Next >** button.
   Ready to Complete page displays.

6. Select the **Finish** button.
   A successful message displays.
EventTracker: Virtual Appliance

Configure 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$126

   **NOTE:**
   On 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 [Update System Name](#) zip file on local drive and extract this file in C:\.

   **NOTE:**
   This is Server core version of OS and windows desktop will not be shown.

5. Run the command prompt as administrator.

6. Execute the batch file **UpdateSystem.bat** in the command prompt.
7. Change the directory to `C:\Program Files (x86)\Prism Microsystems\EventTrackerWeb\bin` folder.

8. Run the executable file `evtInstallConfig.exe` in the command prompt.
9. Update the user credential ETAdmin user or select active directory and enter domain user credential.

10. Once EventTracker Configuration validates the credential and runs successfully, install VMware Tools on newly imported Virtual machine.

11. Change **start up type** 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
   - StatusTracker
   - TrapTracker Receiver
   - WcwService

12. In command prompt, navigate to C:\Program Files (x86)\Prism Microsystems\EventTracker\ folder, and execute the file ETControlPanel.exe.

    EventTracker Control Panel window displays.
13. Double click on License Manager and verify the license.
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 the future reference. Secure the system using strong password.