

EventTracker Log Management (ETLM): Virtual Appliance

Quick Start Guide Version 9.3 Build 5

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.	EventTracker 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	Importing EventTracker Virtual Appliance	6
1.5	Upgrading Virtual Hardware.....	11
1.6	Adding a new Network adapter	12
1.6.1	Removing an existing network interface	12
1.6.2	Adding a new network interface	15
1.7	Configuring EventTracker Virtual Appliance	18

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.

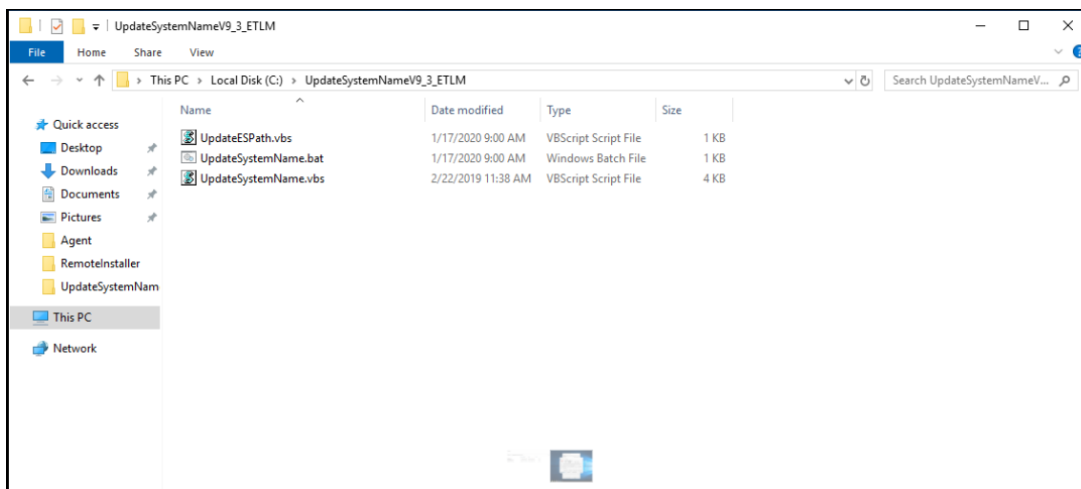


Figure 1

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**.

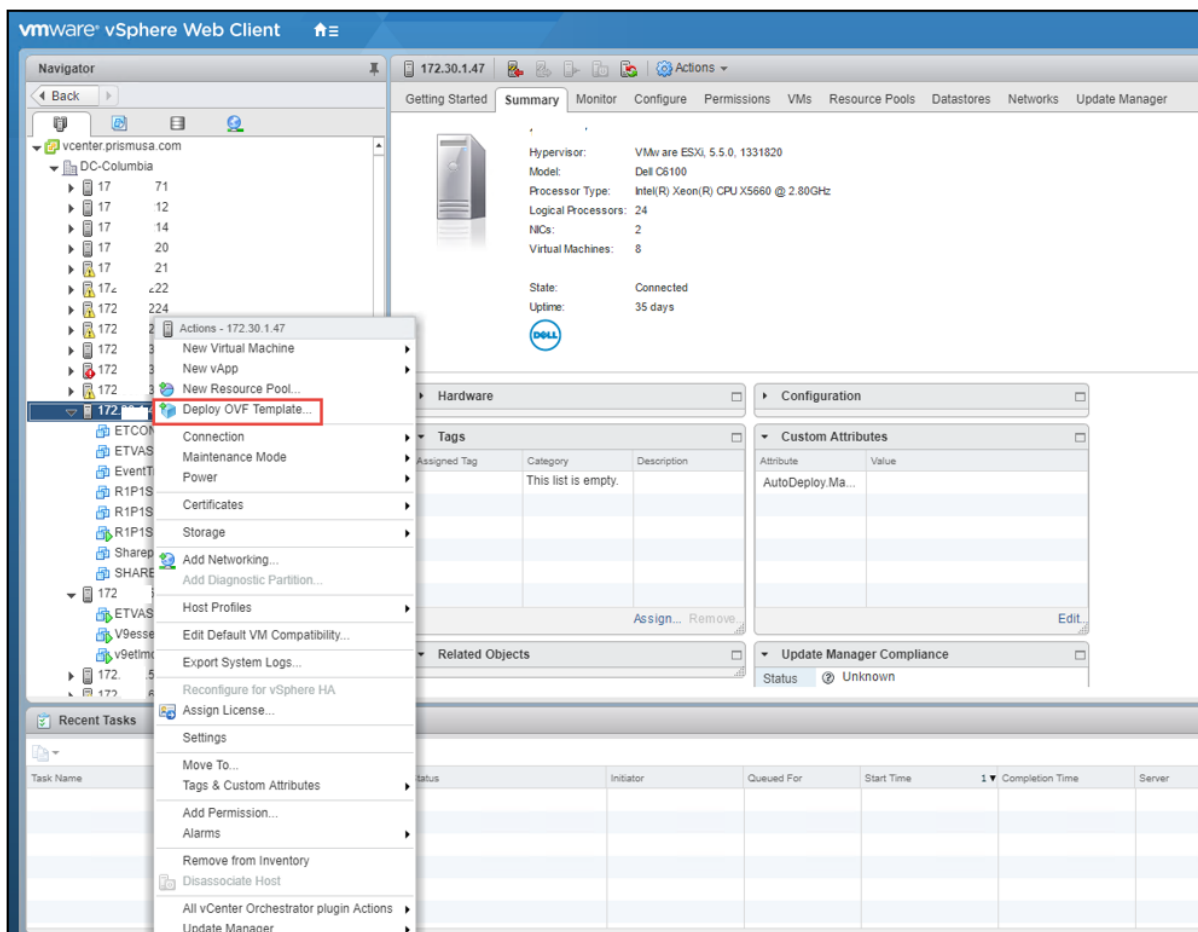


Figure 2

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

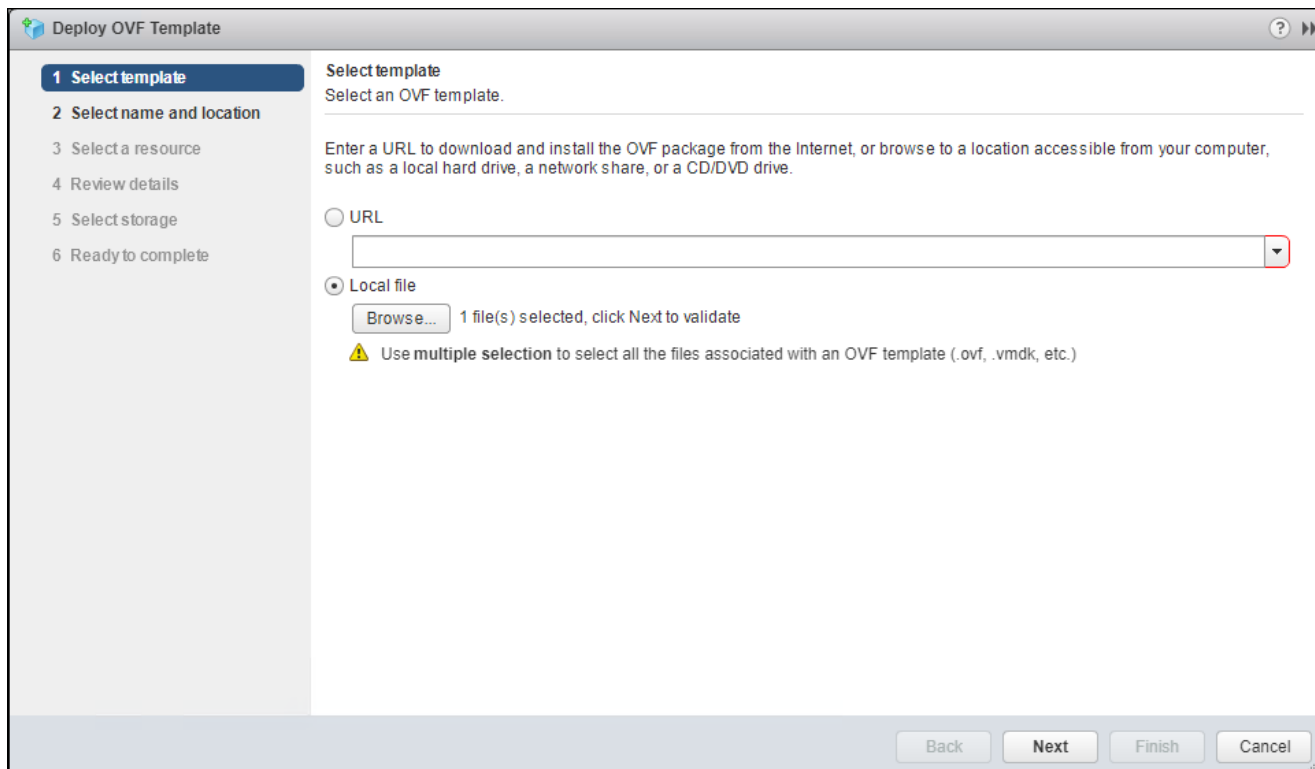


Figure 3

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

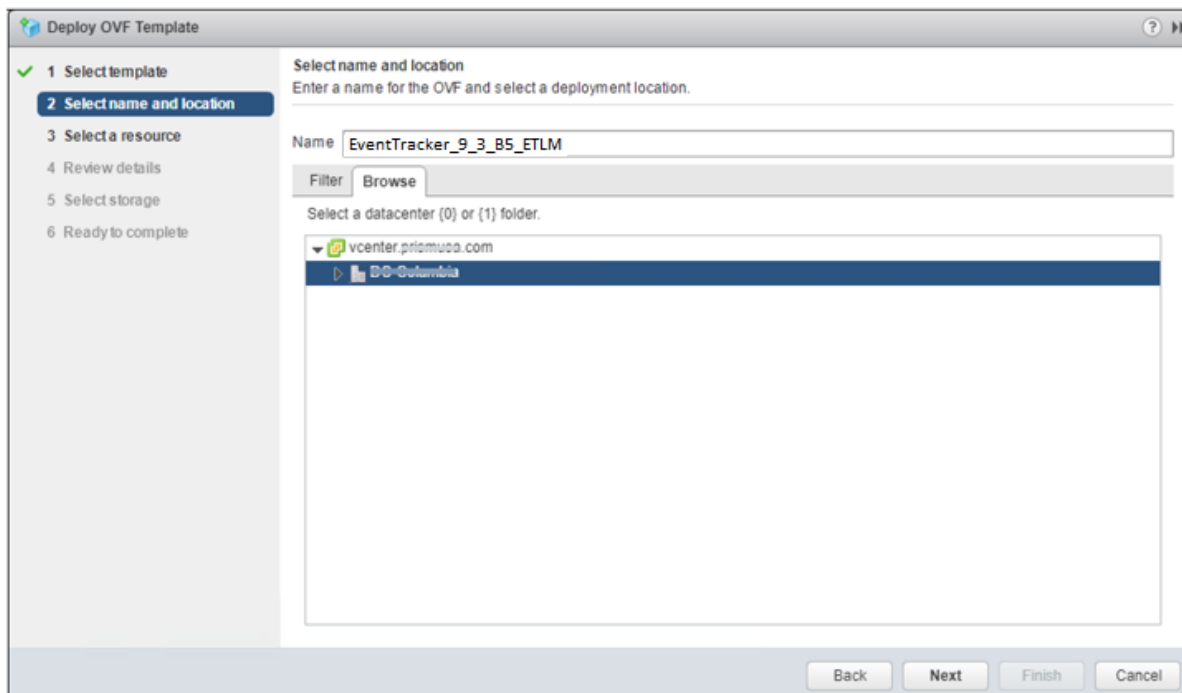


Figure 4

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

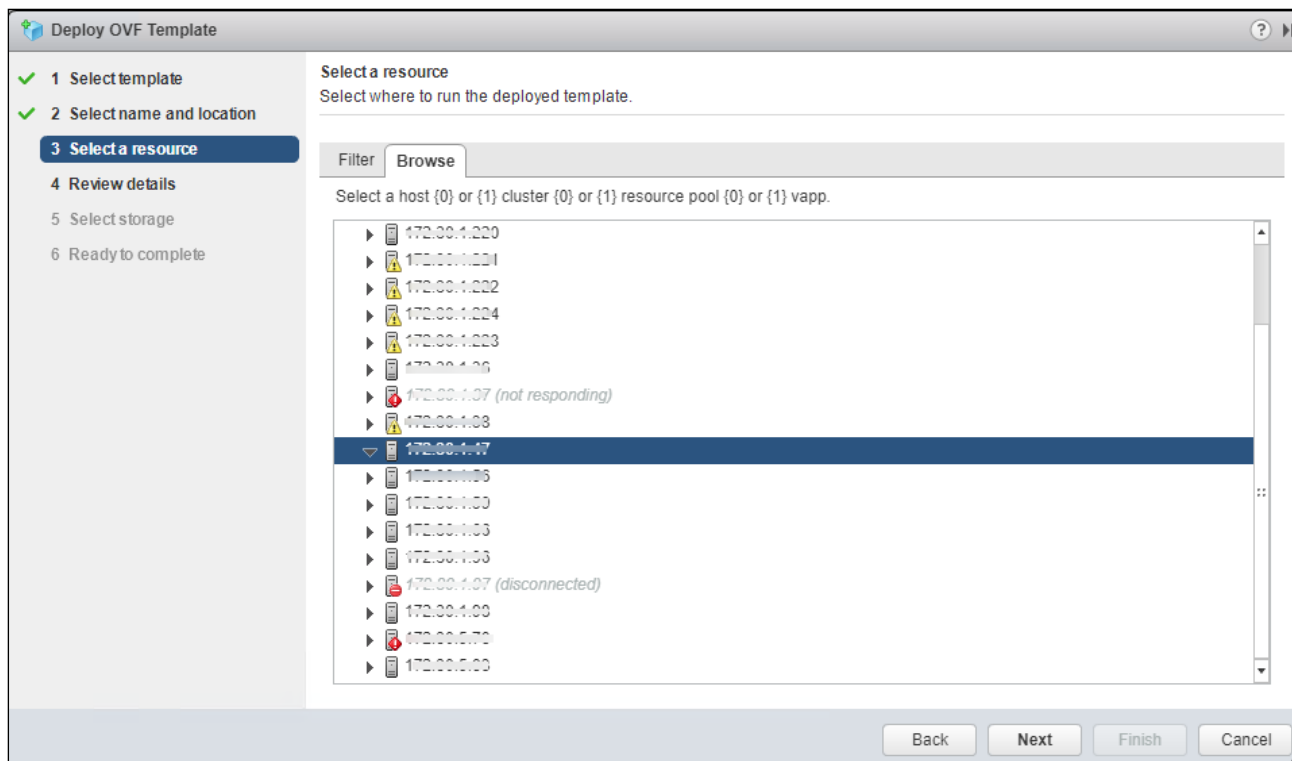


Figure 5

6. Review the details and click **Next** \geq .

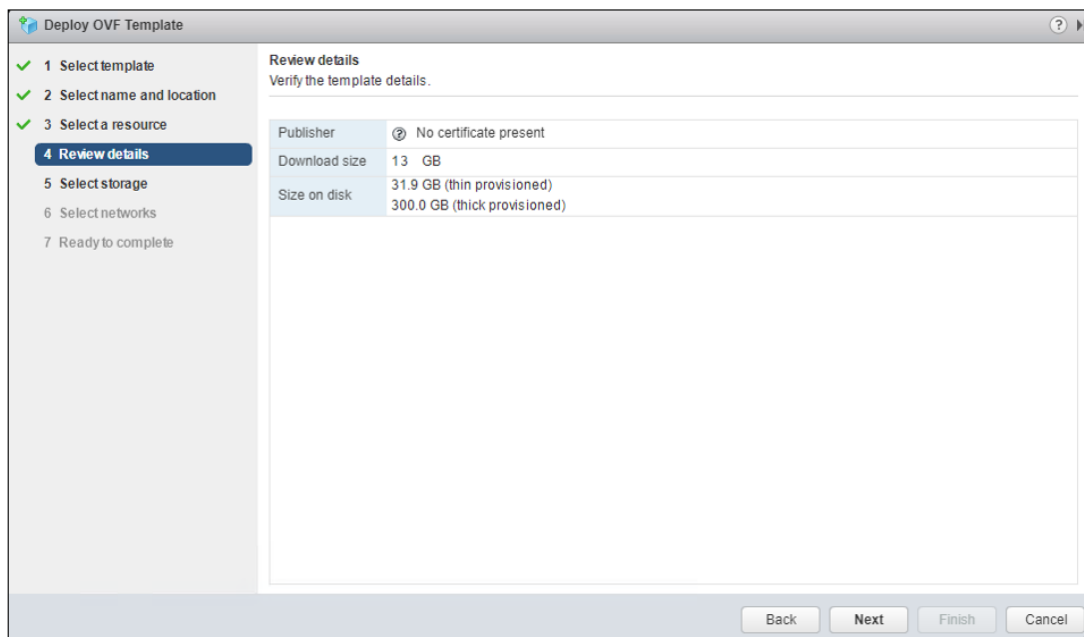


Figure 6

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

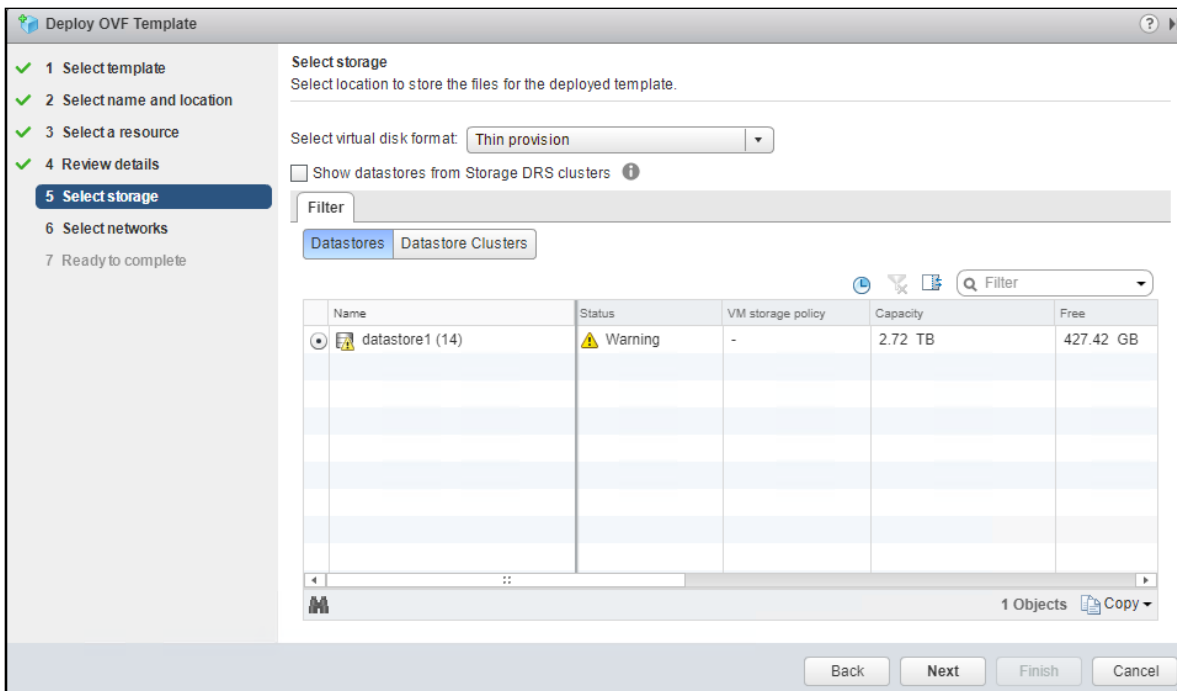


Figure 7

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

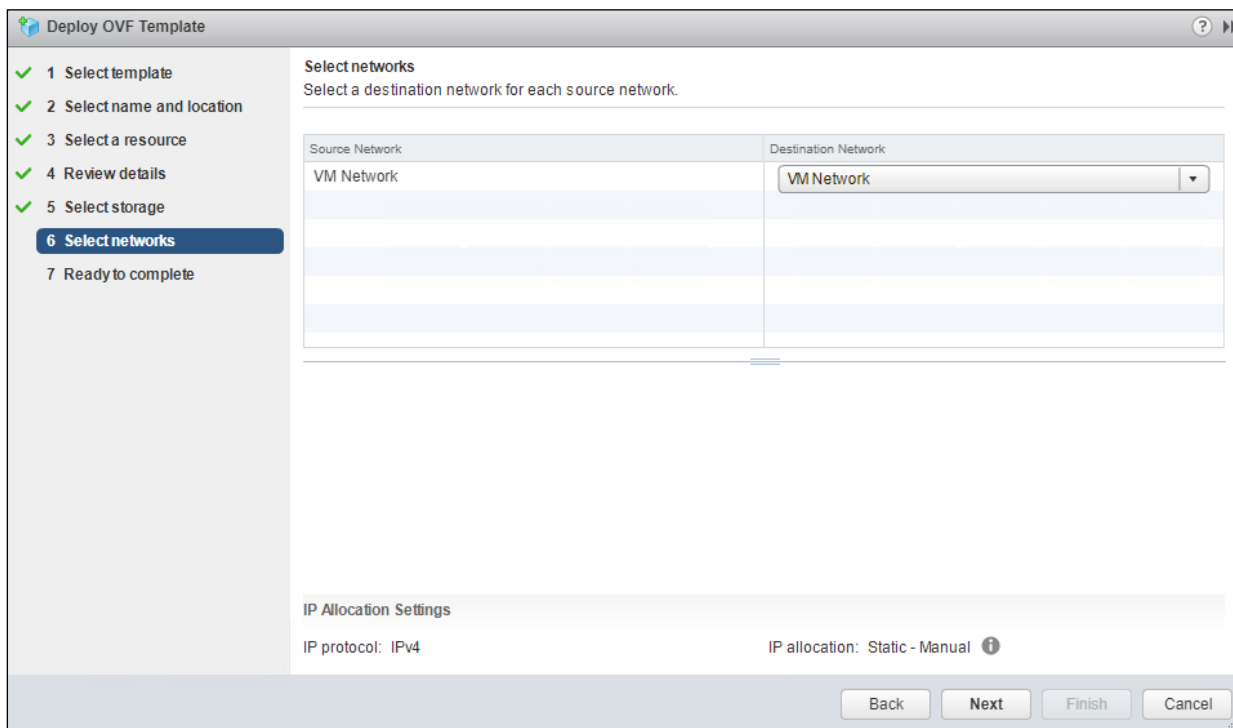


Figure 8

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

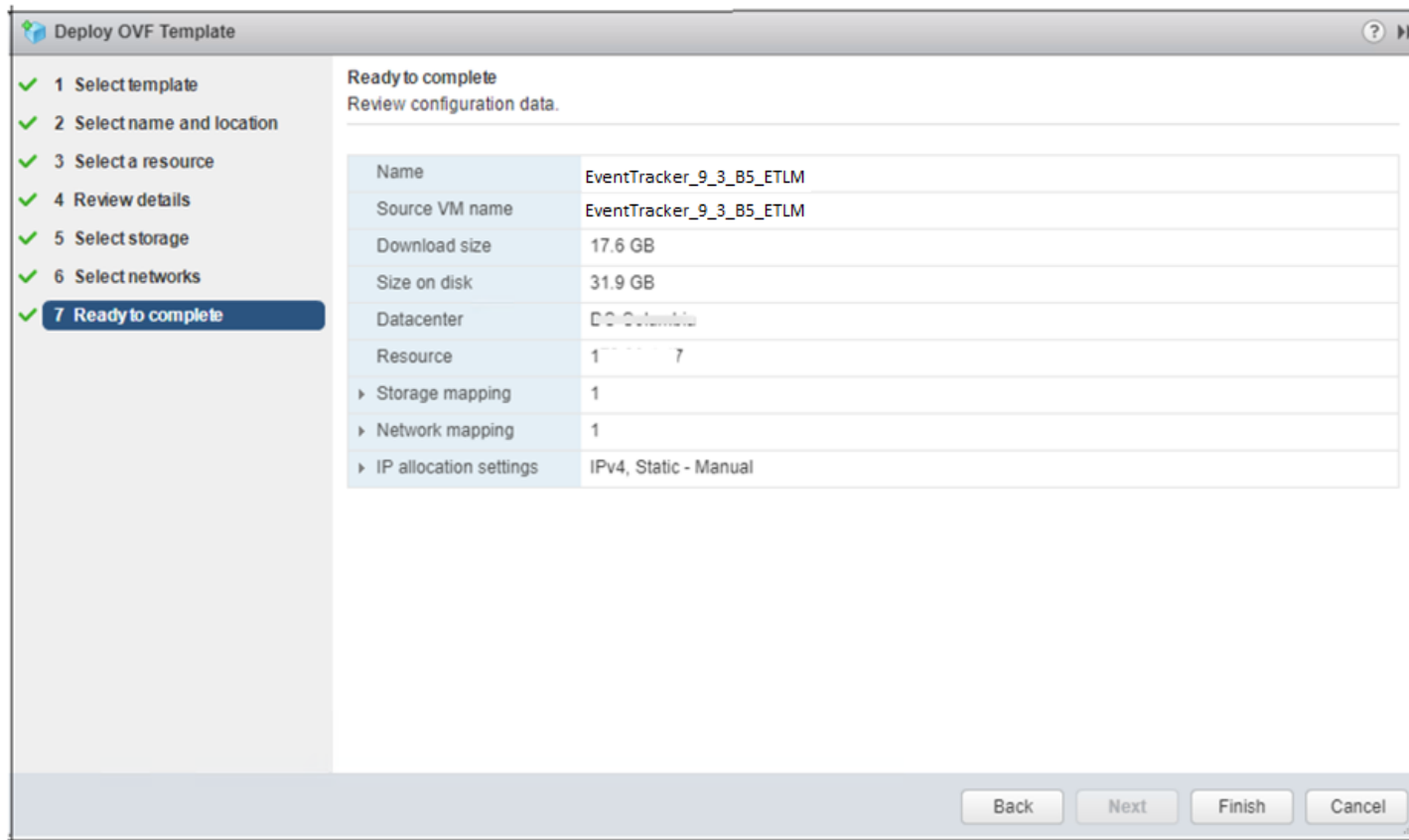


Figure 9

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

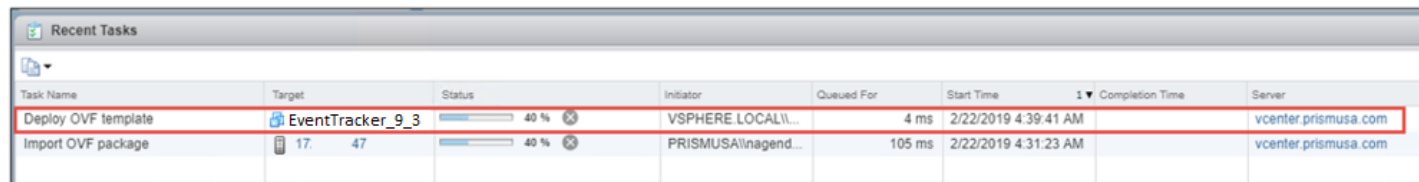


Figure 10

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

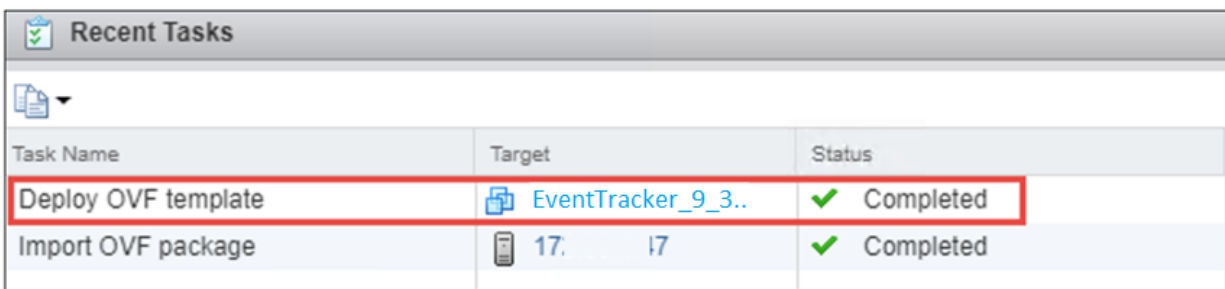


Figure 11

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**.

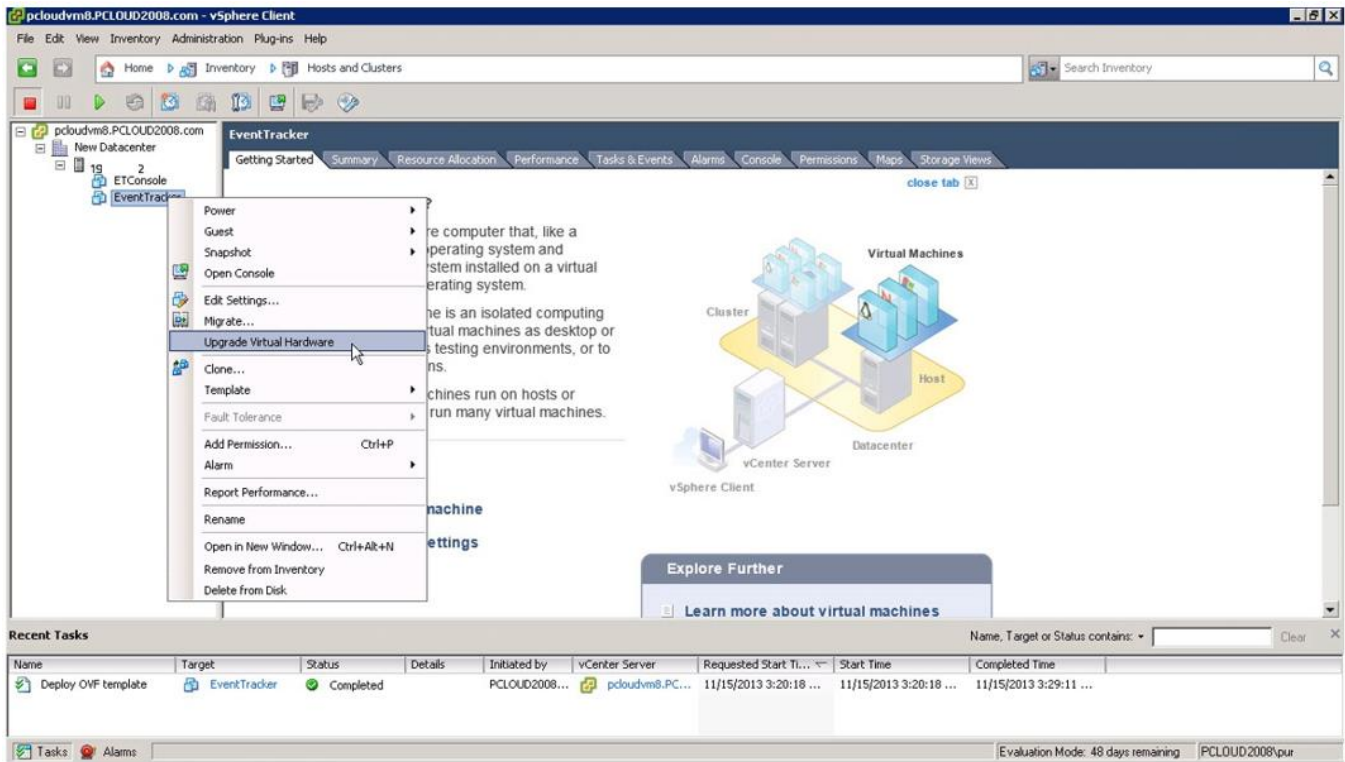


Figure 12

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

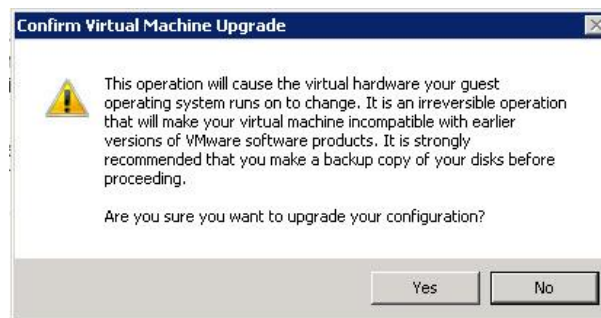


Figure 13

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

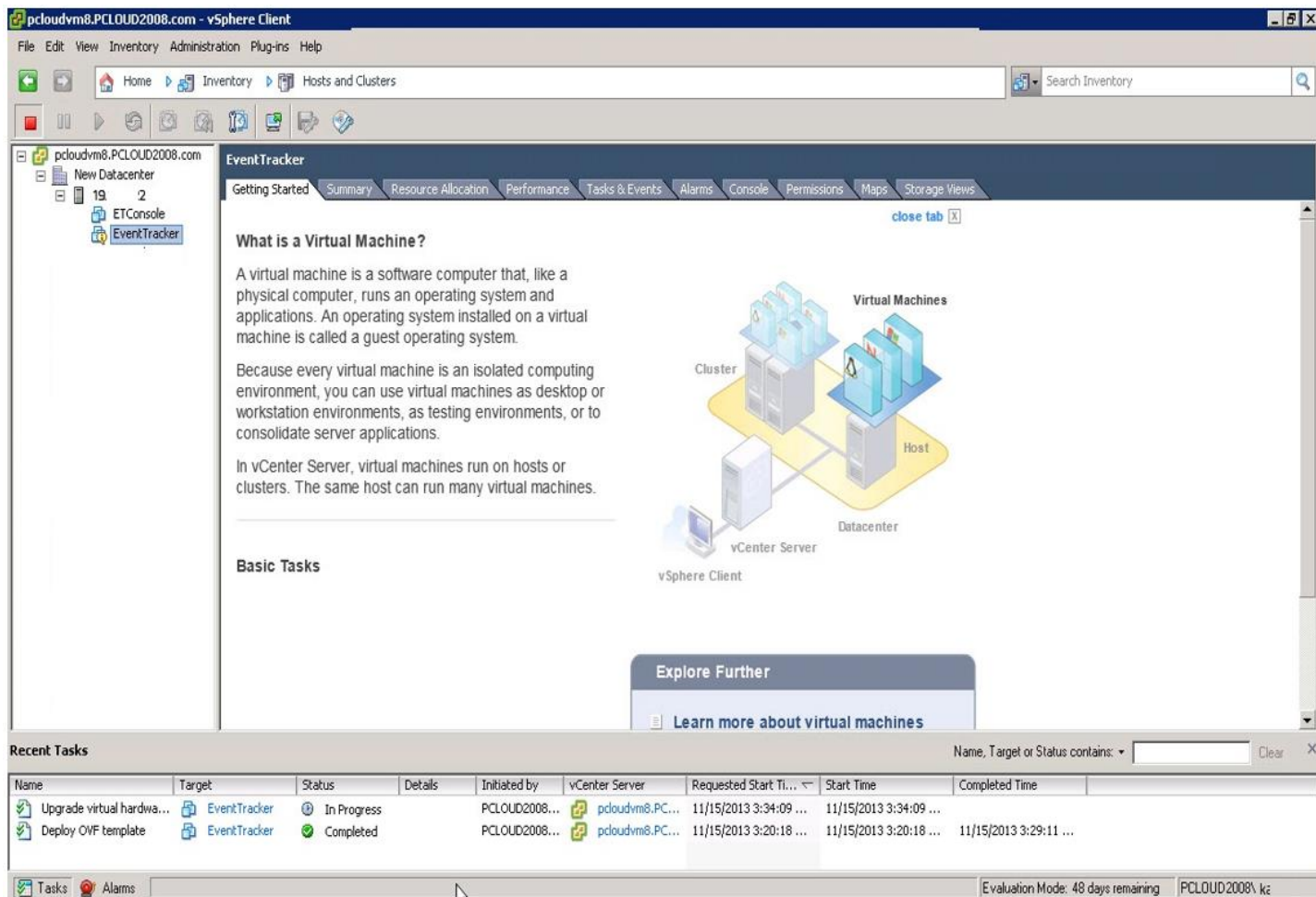


Figure 14

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...**

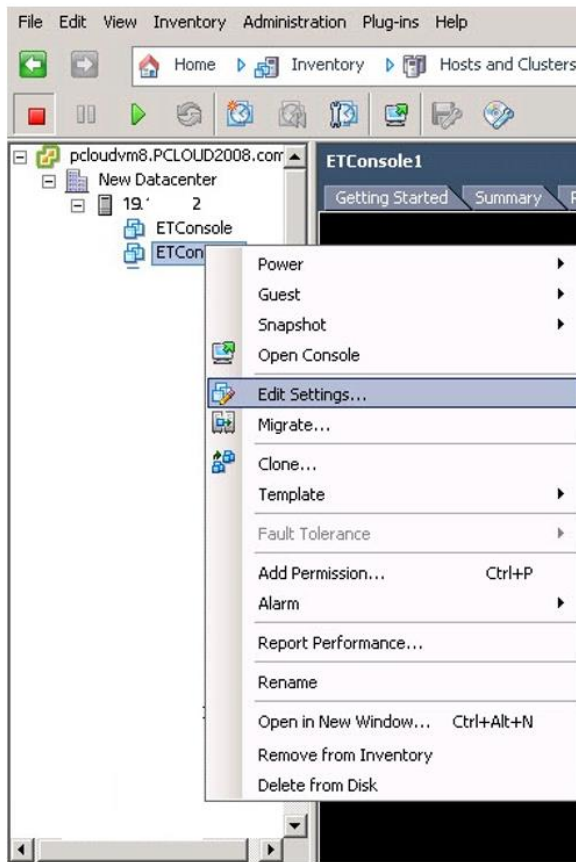


Figure 15

2. Virtual Machine Properties window opens.

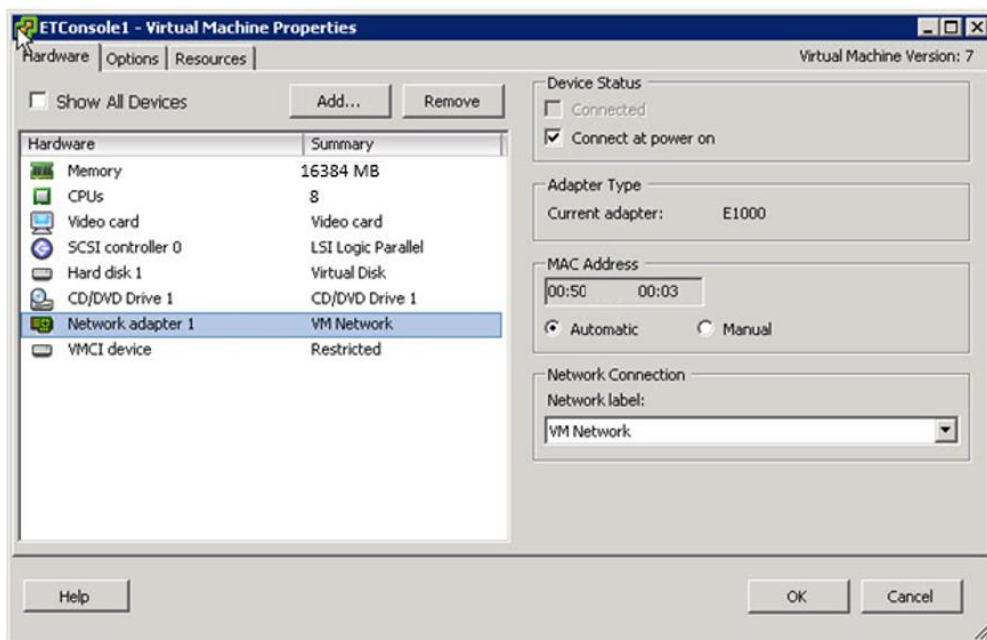


Figure 16

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

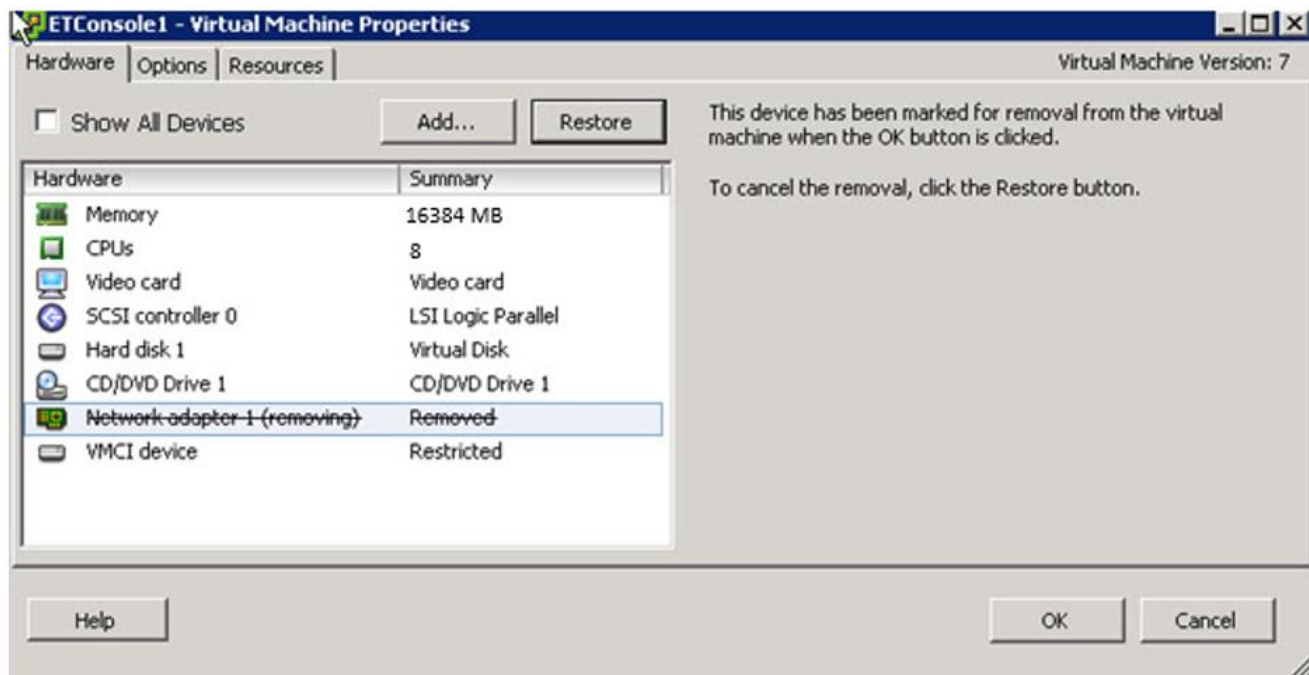


Figure 17

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

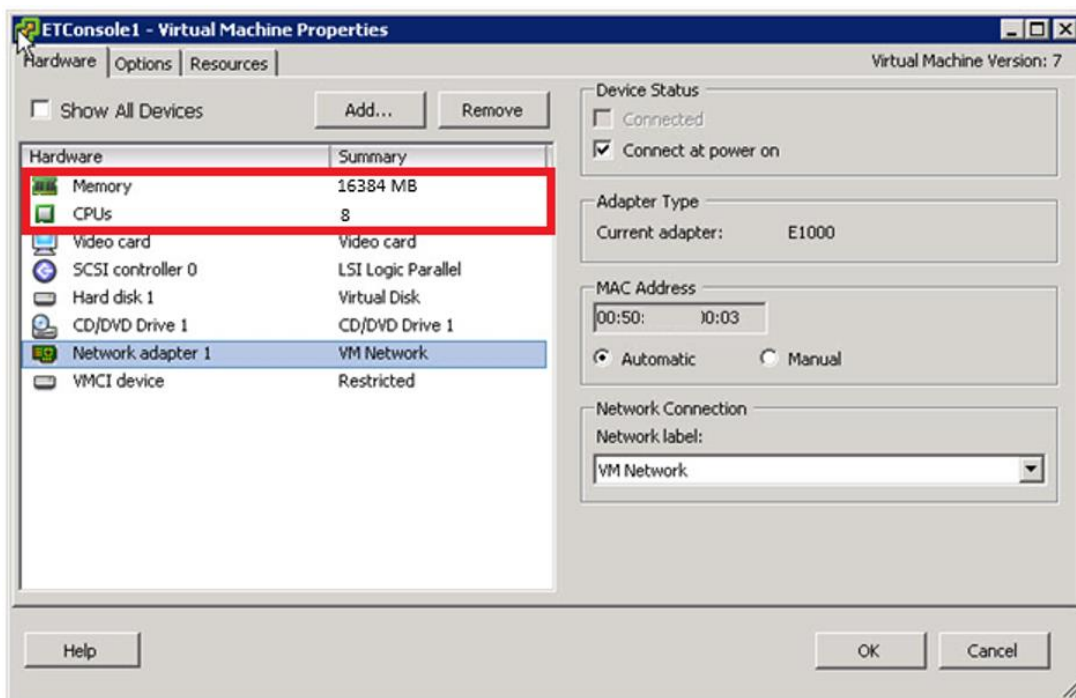


Figure 18

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.

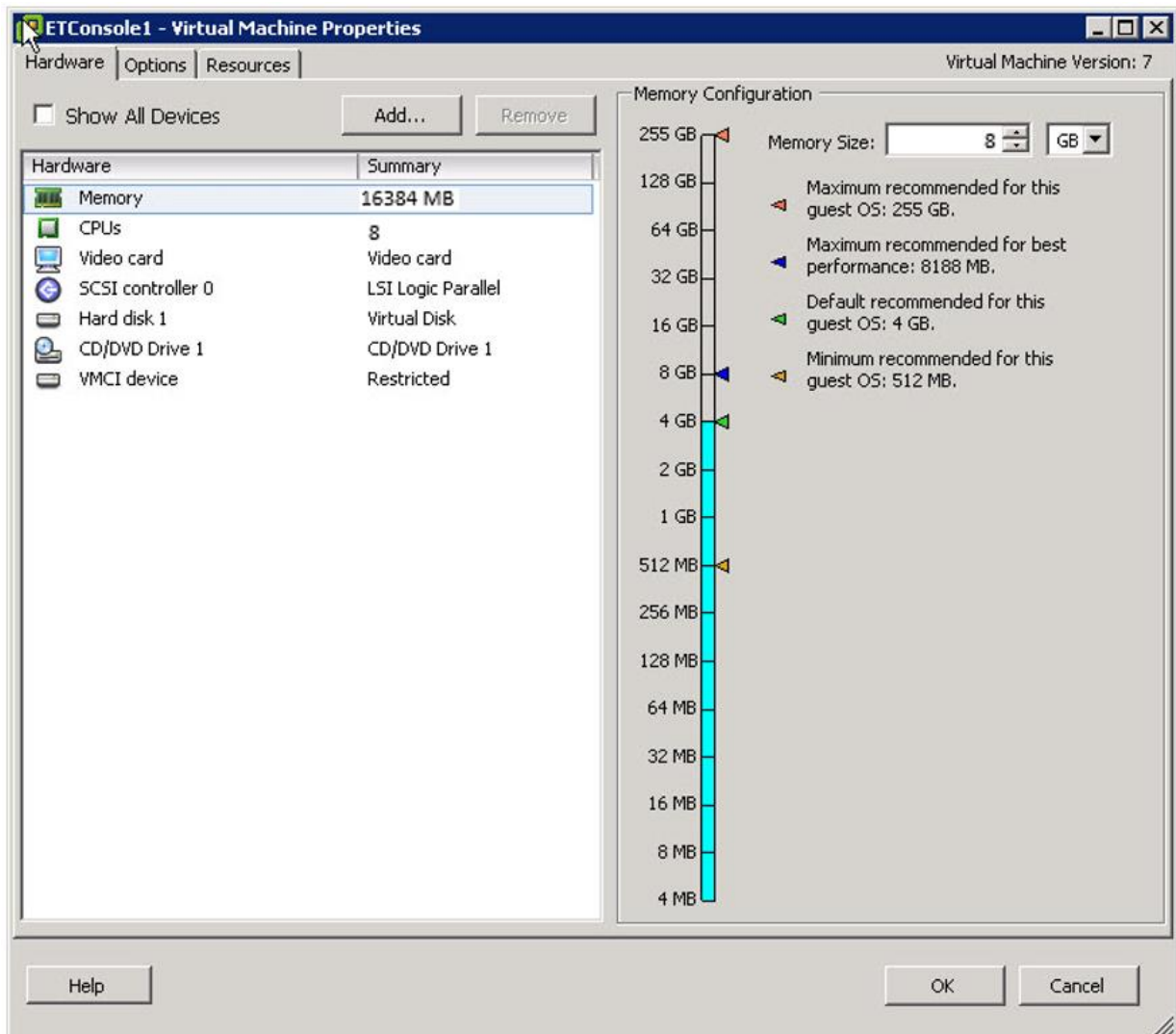


Figure 19

2. Select **Add...**
Add Hardware window opens.

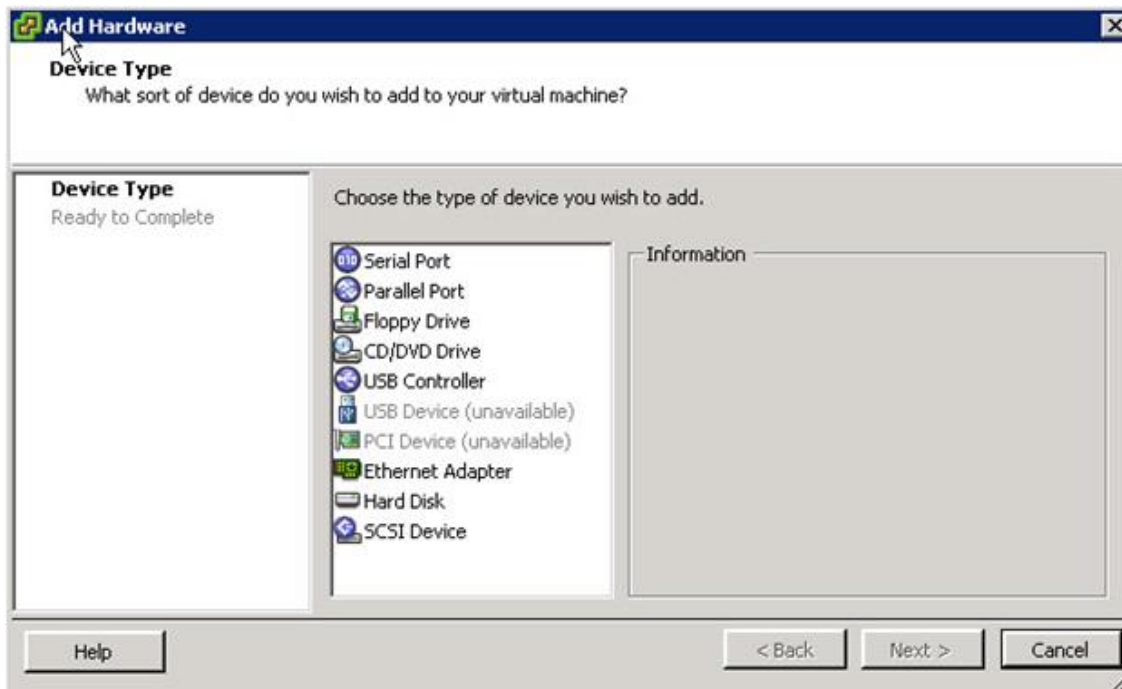


Figure 20

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

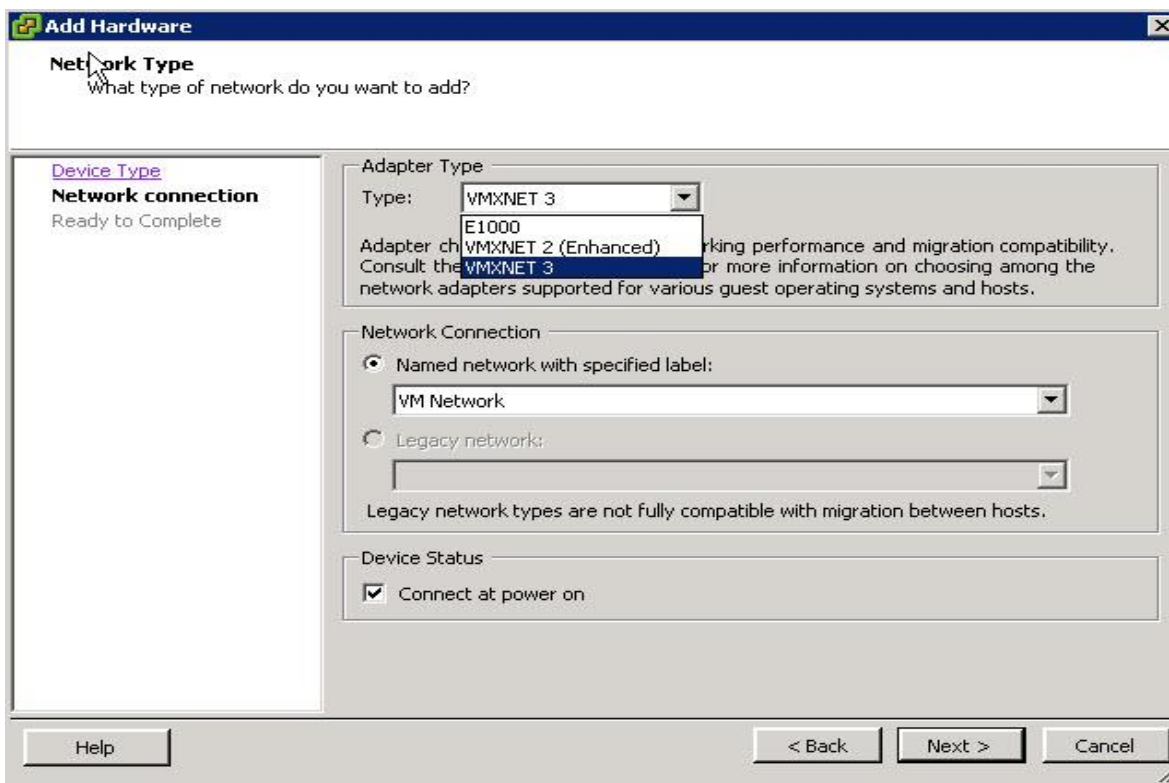


Figure 21

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.

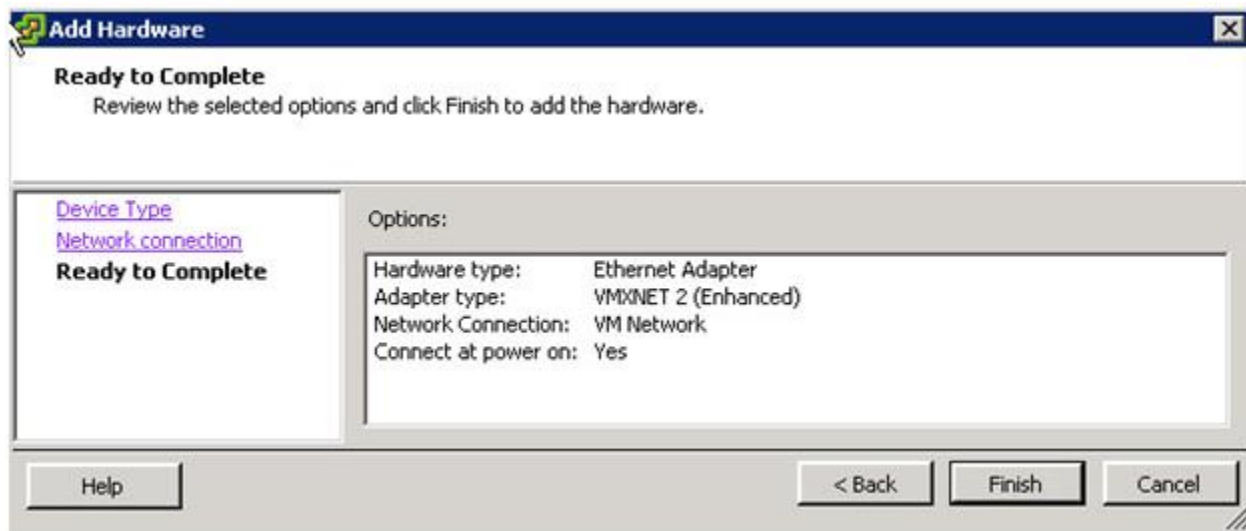


Figure 22

6. Click **Finish**.
A successful message opens.

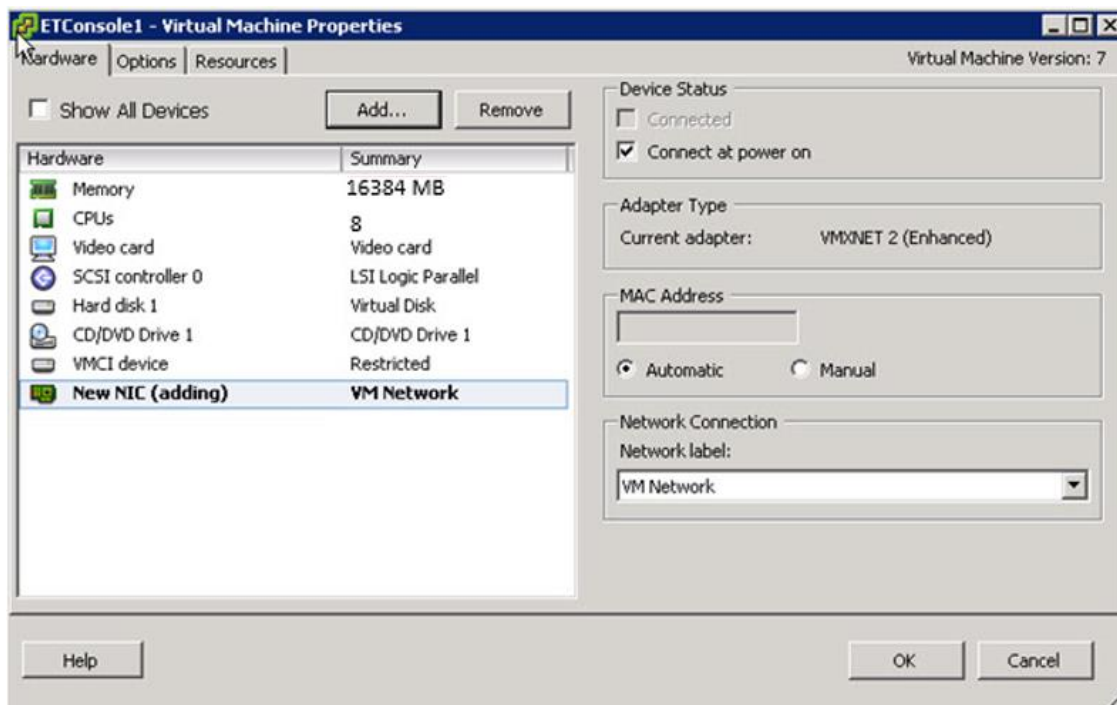


Figure 23

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.

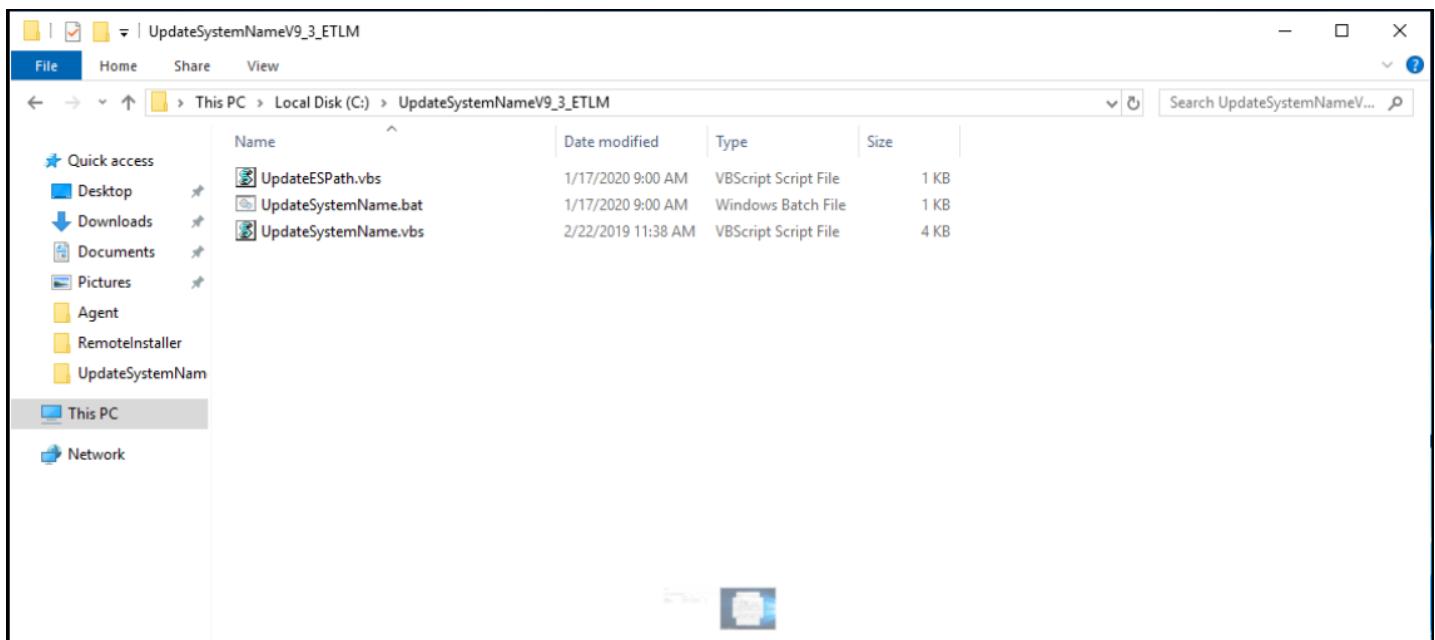


Figure 24

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

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

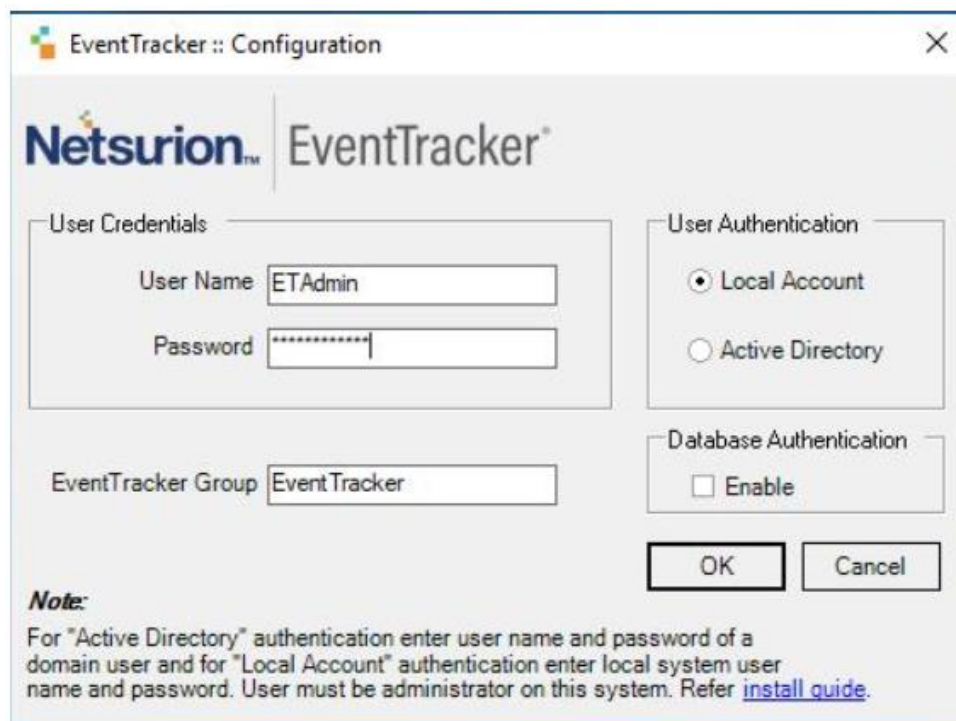


Figure 25

- Update the user credential ETAdmin user or select an active directory and enter domain user credentials.
- Once **EventTracker Configuration** validates the credential and runs successfully, install **VMware Tools** on newly imported Virtual machine.
- 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.

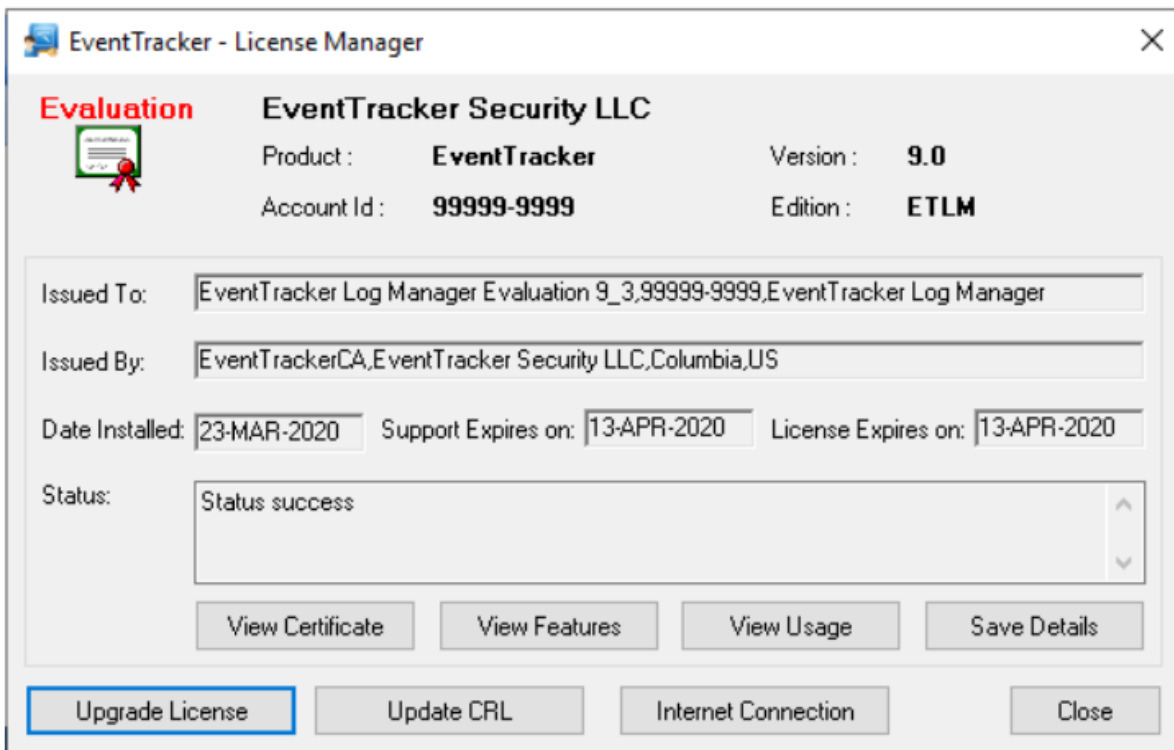


Figure 27

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 all
DNS Name:	pcloud37-vm7.PCLOUD2008.com
State:	Powered On
Host:	pcloud37.prismusa.com
Active Tasks:	
vSphere HA Protection:	 N/A 

Figure 28