

## 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

<b>1</b>	<b>EventTracker Virtual Appliance in VMWare Environment .....</b>	<b>4</b>
1.1	Minimum Hardware Requirements.....	4
1.2	EventTracker Virtual Appliance Details .....	4
1.3	Prerequisites.....	5
1.3.1	Summary.....	5
1.4	Setting up EventTracker Virtual Appliance.....	6
1.4.1	Installing EventTracker Virtual Appliance.....	6
1.4.2	Importing EventTracker Virtual Appliance .....	7
1.5	Upgrading Virtual Hardware.....	12
1.6	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	Configuring EventTracker Virtual Appliance.....	19

# 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

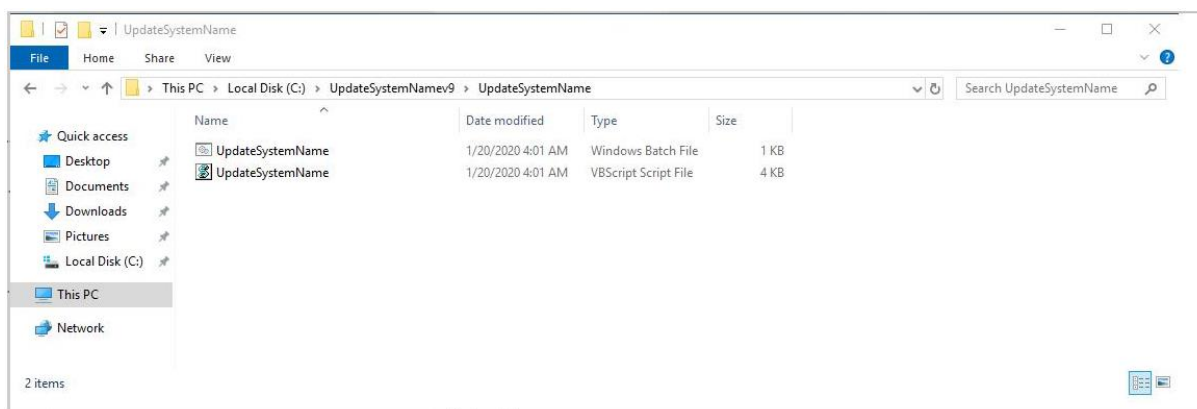
- **EventTracker OVF file size** – 12.6 GB
- **Hostname** – ETConsole
- **WorkGroup** – EventTracker
- **Disk Space:** 300 GB (33 GB initial)
- **CPU** – 8 Core @2.5 GHz minimum
- **Memory** – 16 GB
- **VM Hard Drive** – SCSI/SSD type
- **IP Address** – Assign Static IP address
- **Operating System** – 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

- 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.

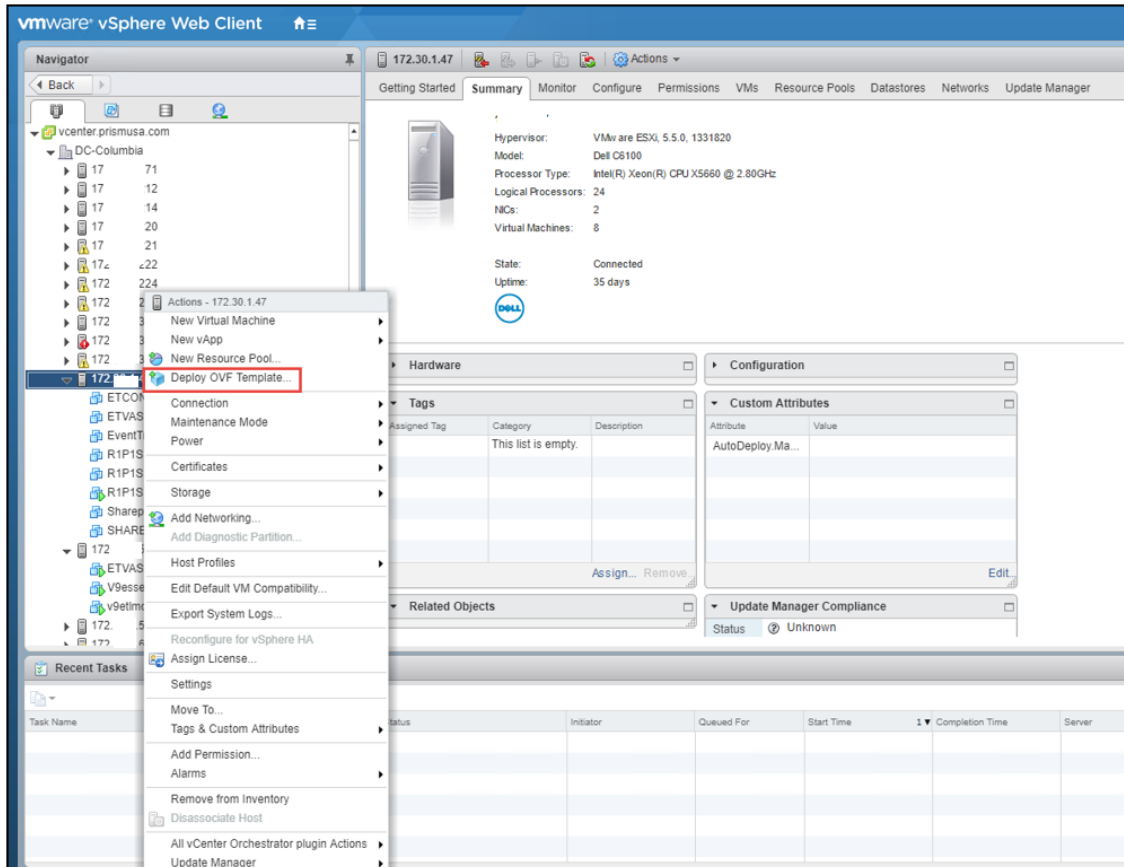
## 1.4 Setting up EventTracker Virtual Appliance

### 1.4.1 Installing EventTracker Virtual Appliance

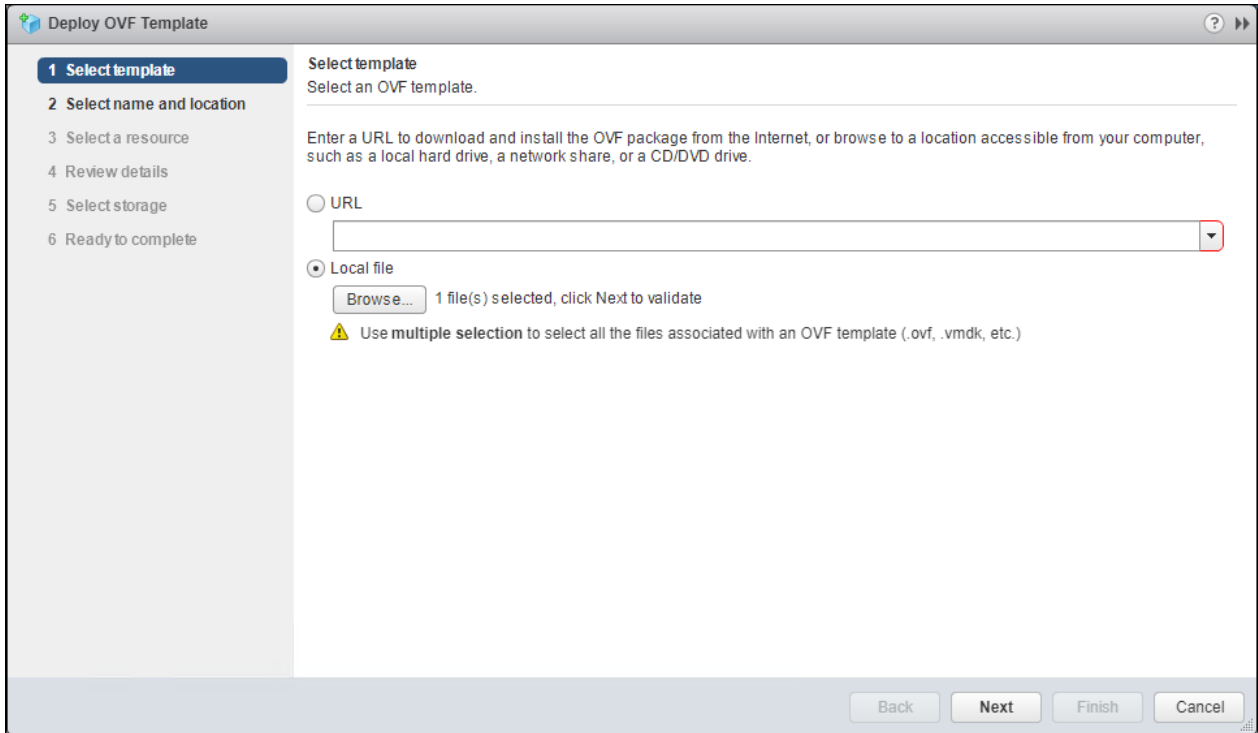
1. Ensure to use fully functional VMware ESX/ESXi 5.5 or later.
2. Get EventTracker Evaluation license from the EventTracker support.
3. Download the '.ova' file from the link provided by the EventTracker technical support.
4. Follow the instructions provided in a detailed section (Import EventTracker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

## 1.4.2 Importing EventTracker Virtual Appliance

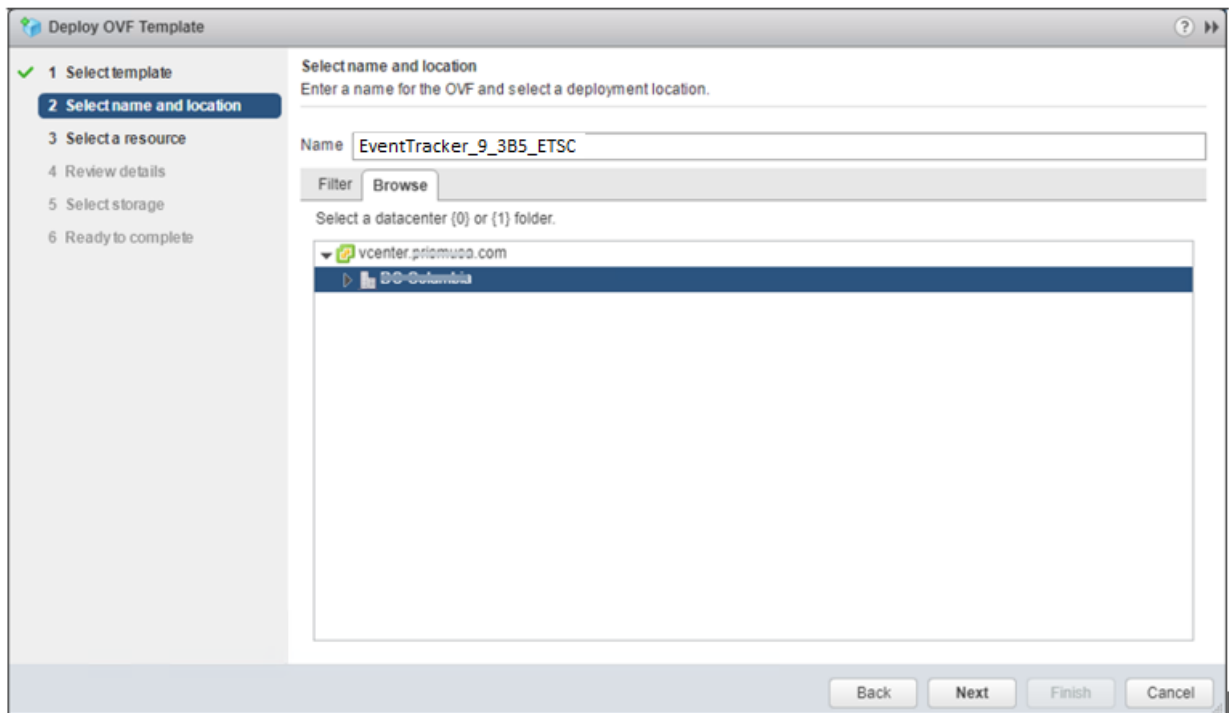
1. Log in to the VMWare VCenter console and select the host.
2. In the **vSphere Web Client**, click the **File** menu, and select **Deploy OVF Template**.



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

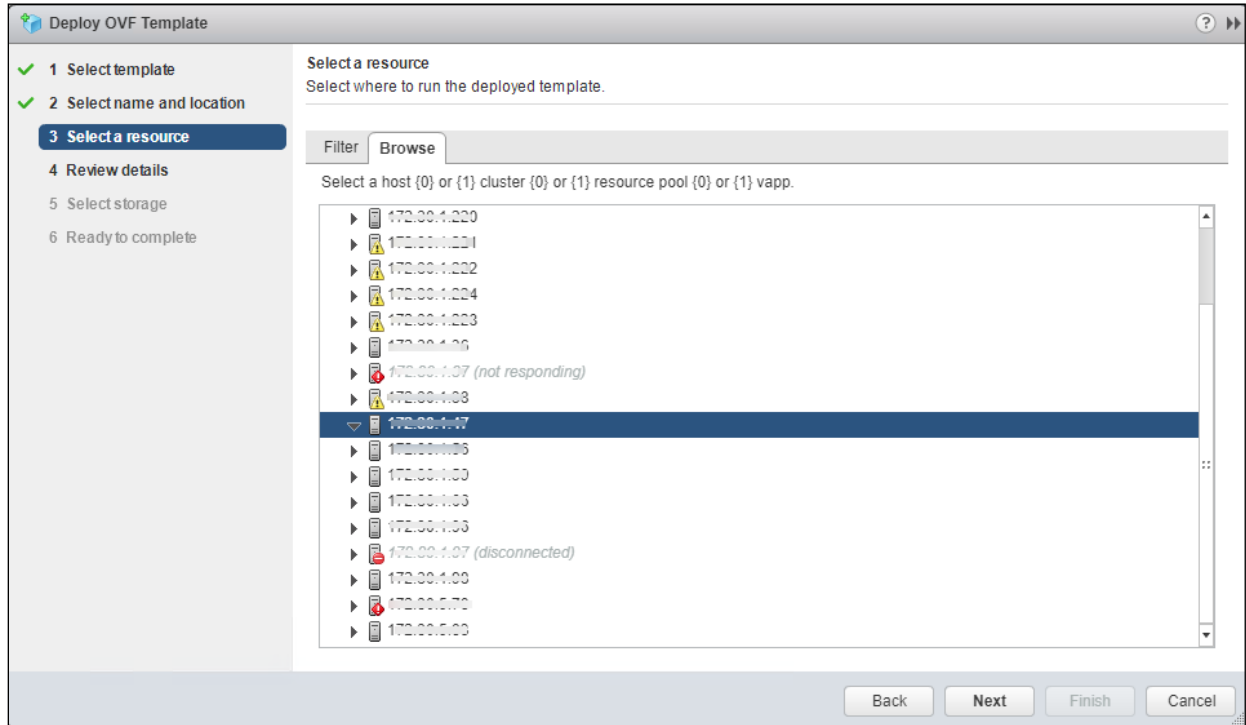


4. Select the name and location and click **Next** >.

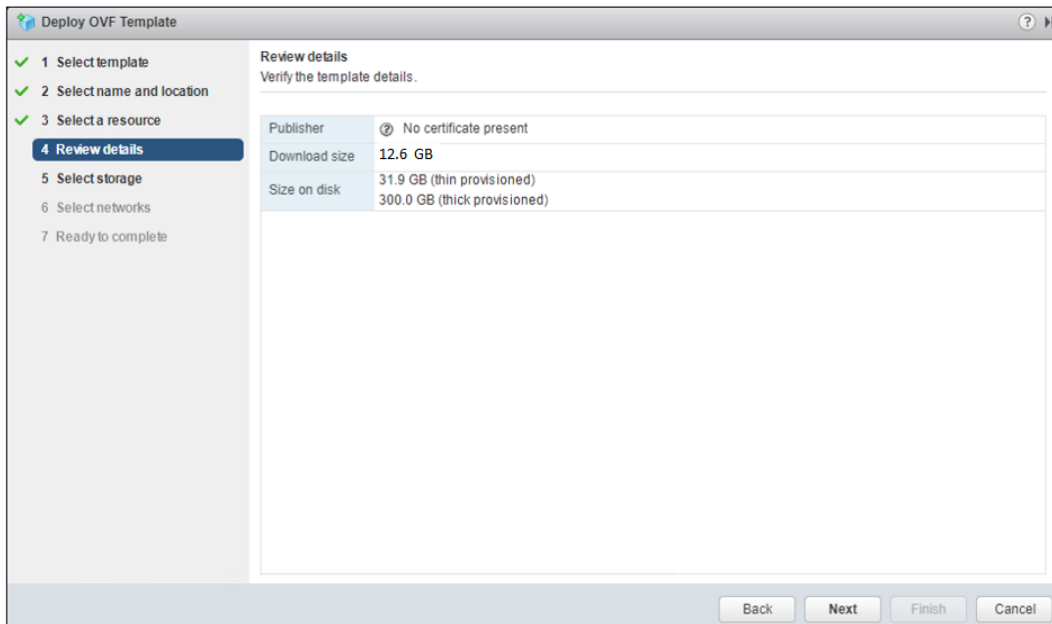




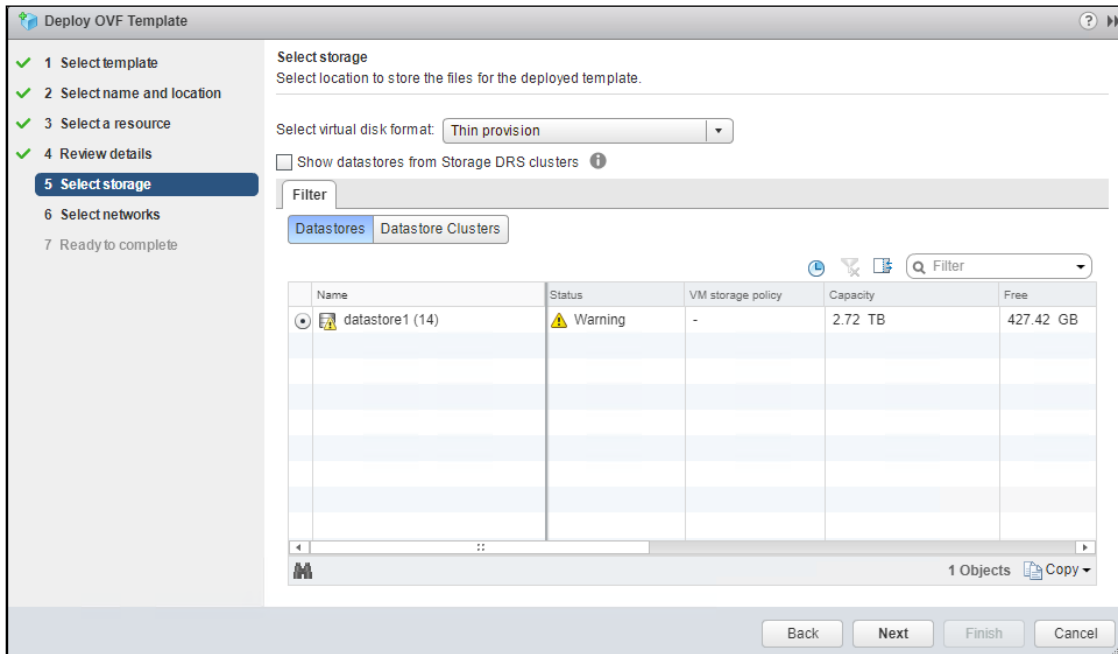
5. Select the host where you want to run the deployment and click **Next** >.



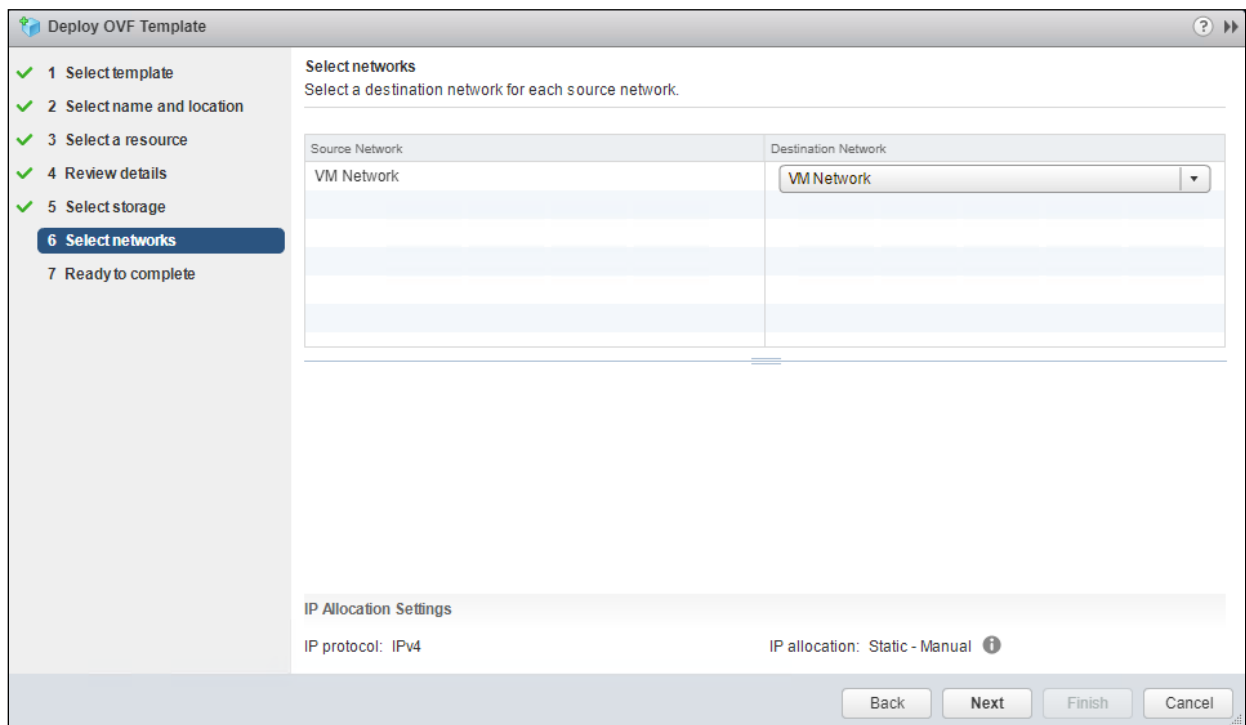
6. Review the details and click **Next** >.



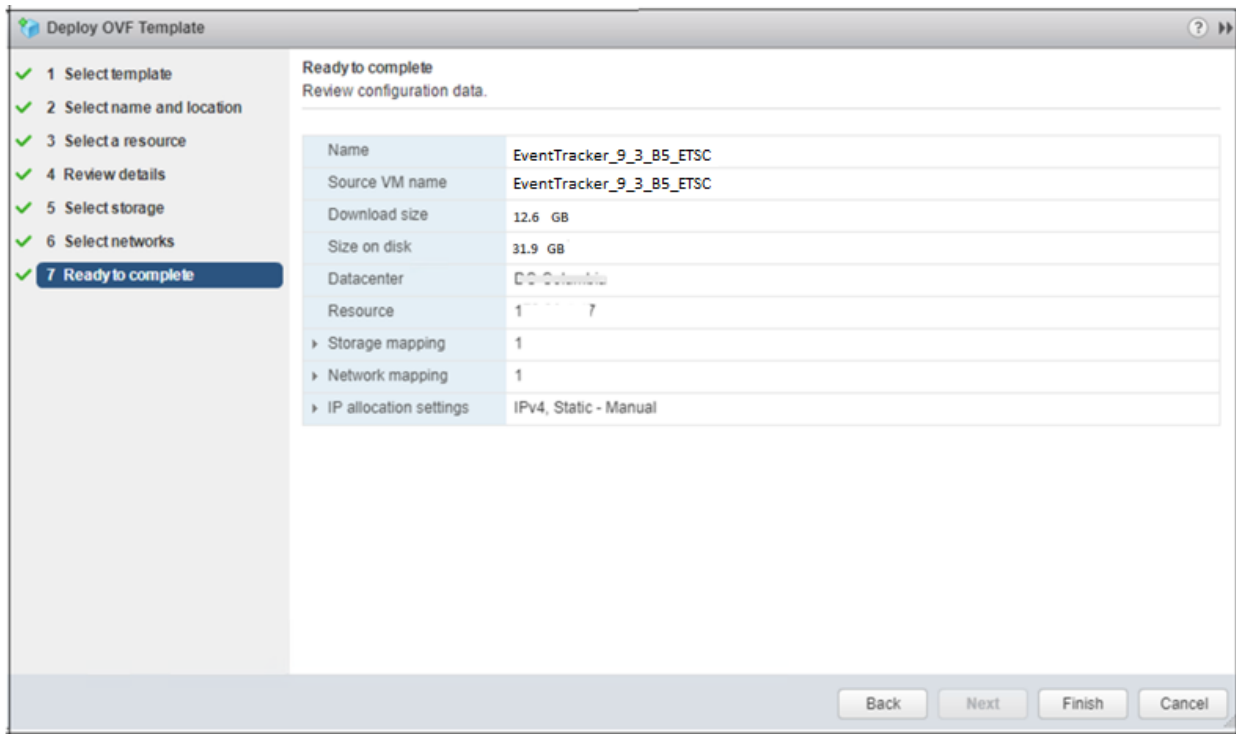
7. To store the virtual disks, select the disk format as **Thin Provision format** and click **Next** >.



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



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



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

Task Name	Target	Status	Initiator	Queued For	Start Time	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\Inagend...	105 ms	2/22/2019 4:31:23 AM		vcenter.prismusa.com

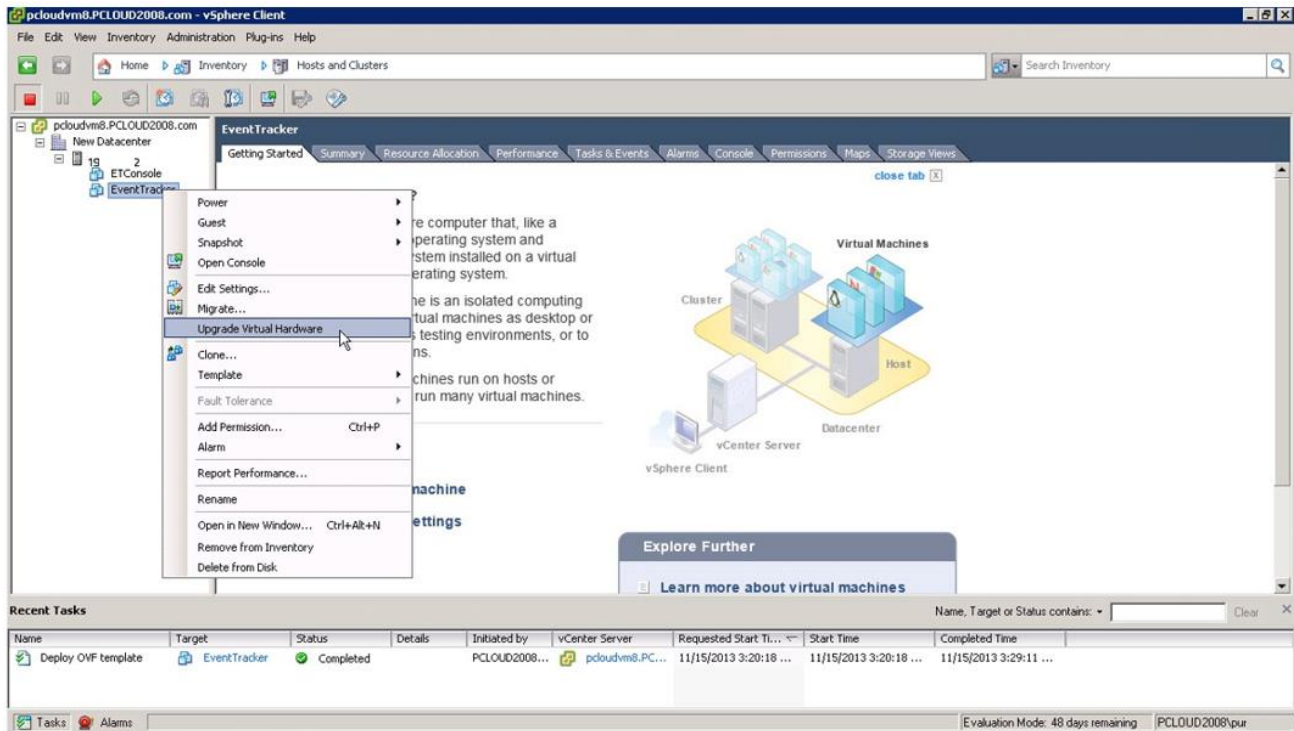
11. After the deployment is completed, it displays the status as **“Completed”**.

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**.

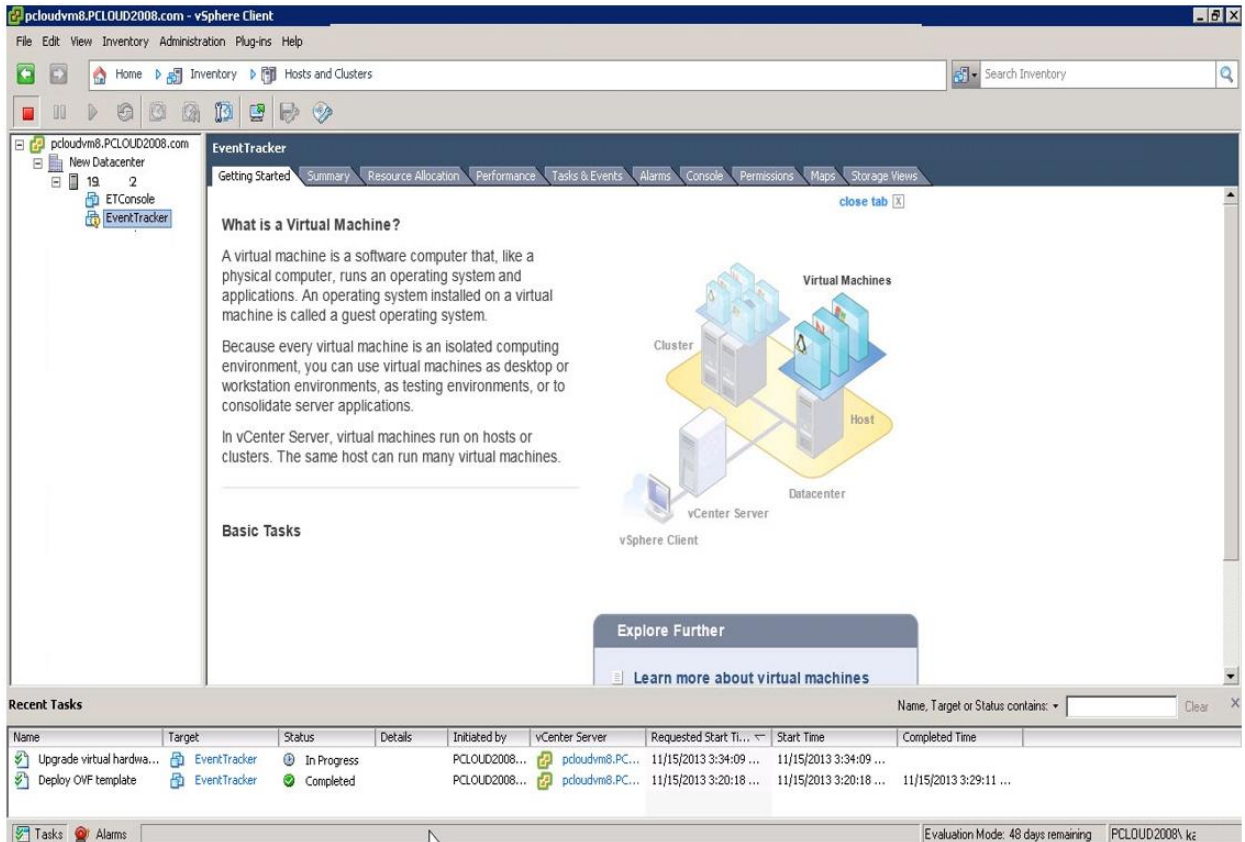


A warning message displays to confirm the Virtual Machine Upgrade.

2. Click Yes.



- In **Recent Tasks** pane, a message display stating the upgrade is 'In Progress' status.

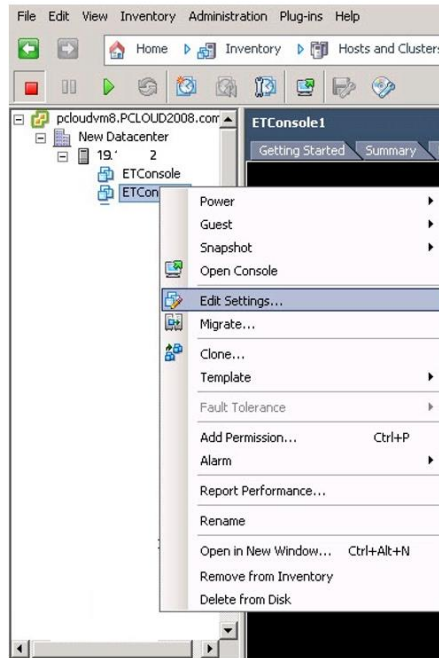


## 1.6 Adding a new Network adapter

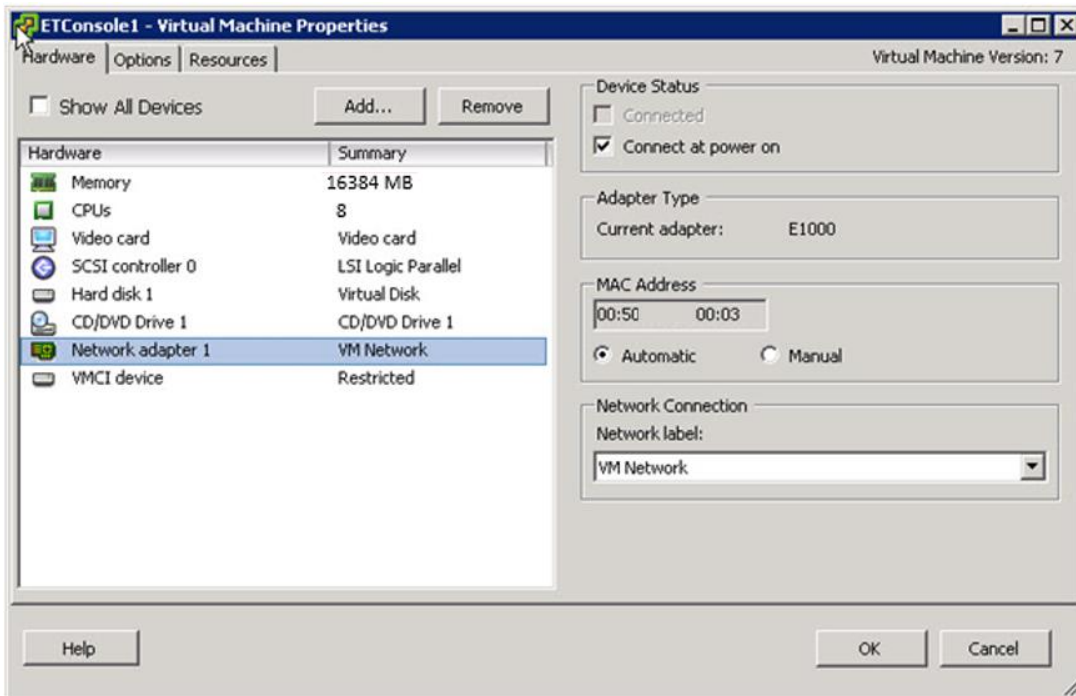
The network adapter provides backward compatibility. After deploying OVA, the user can edit VMware and remove the existing network interface. Later a new network interface is added by selecting the Interface type VMXNET 2 (Enhanced) or VMXNET 3 depending on VMware ESX version.

## 1.6.1 Removing an existing Network Interface

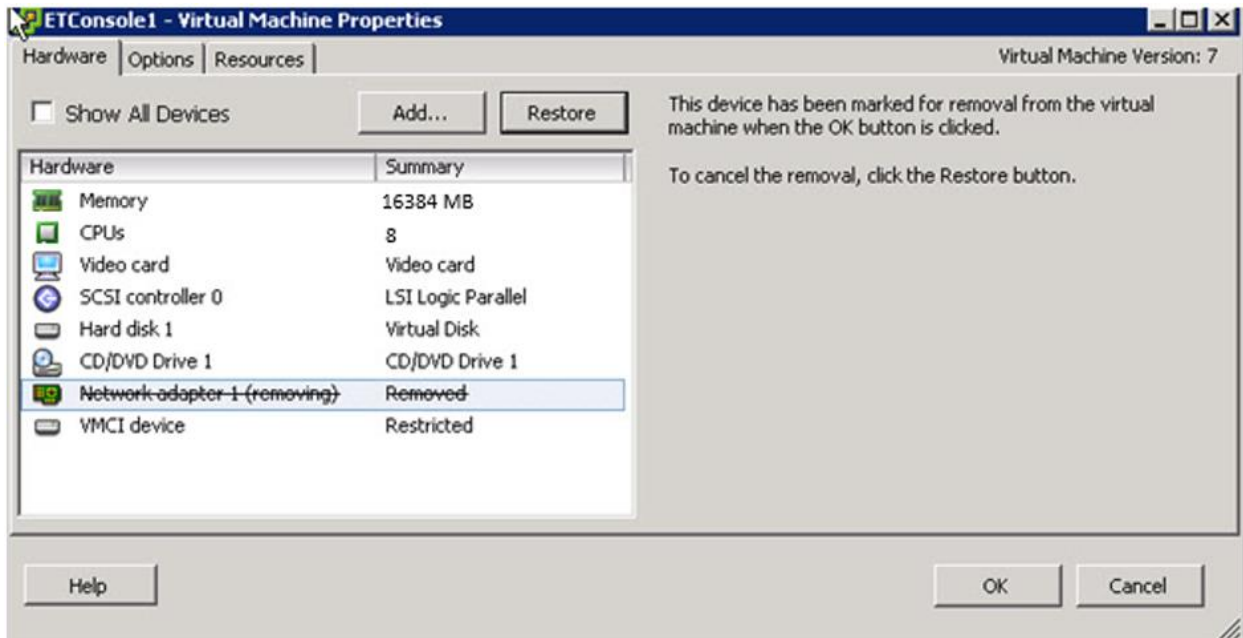
1. To remove an existing network interface, right-click on the machine and select **Edit Settings**.



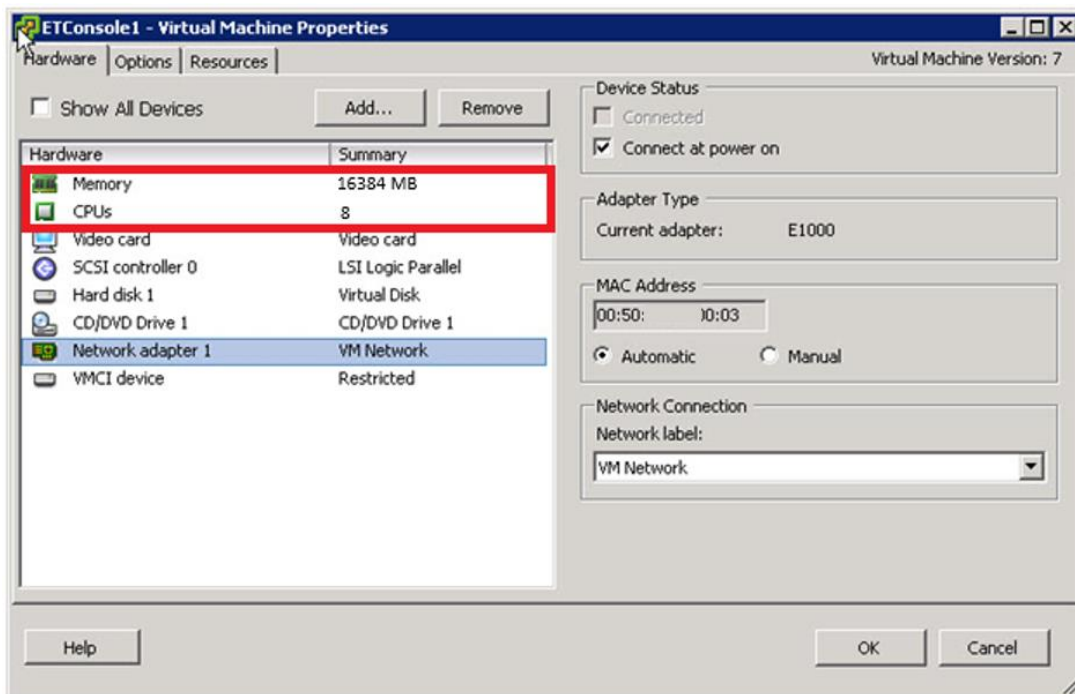
2. **Virtual Machine Properties** window displays.



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



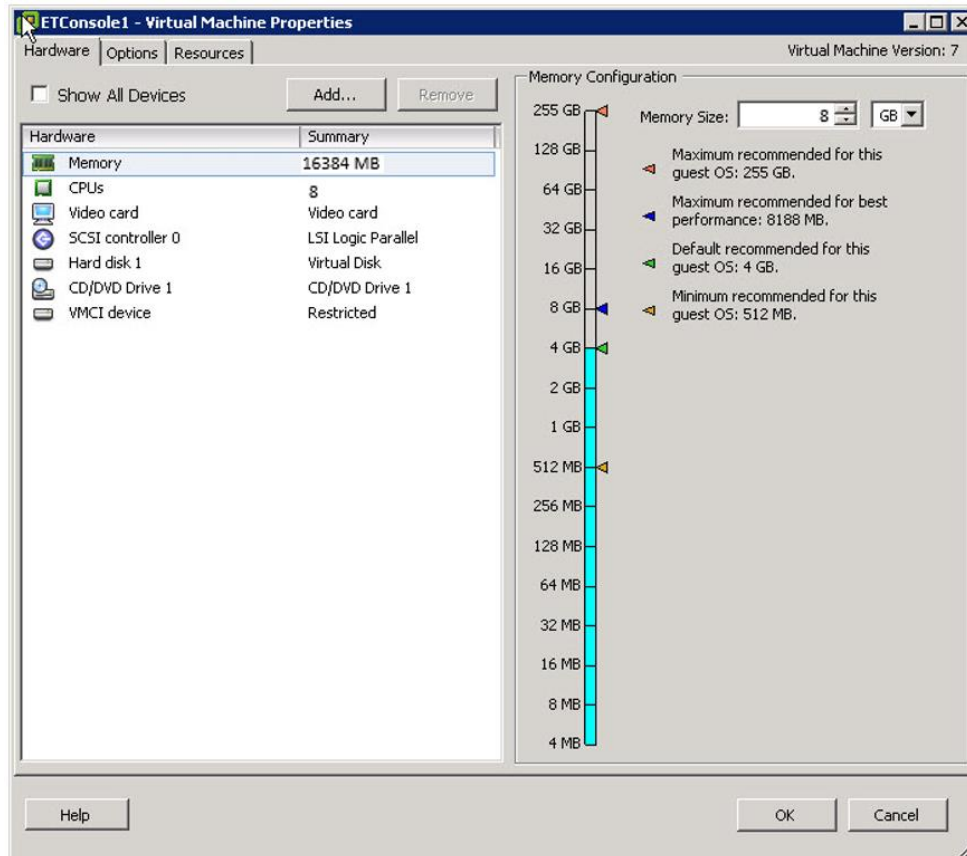
**Note:** The memory and the CPU need to be set according to our standard mentioned in the [requirements](#) page.



## 1.6.2 Adding a new Network Interface

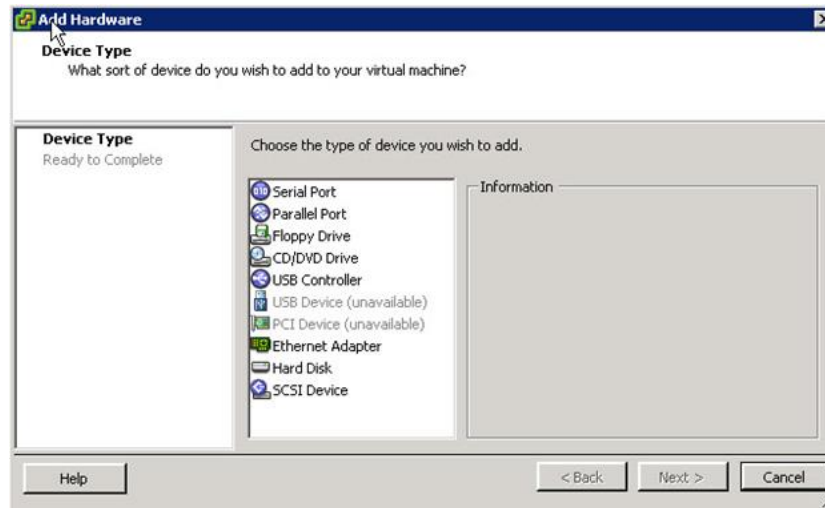
To add an enhanced network adapter,

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

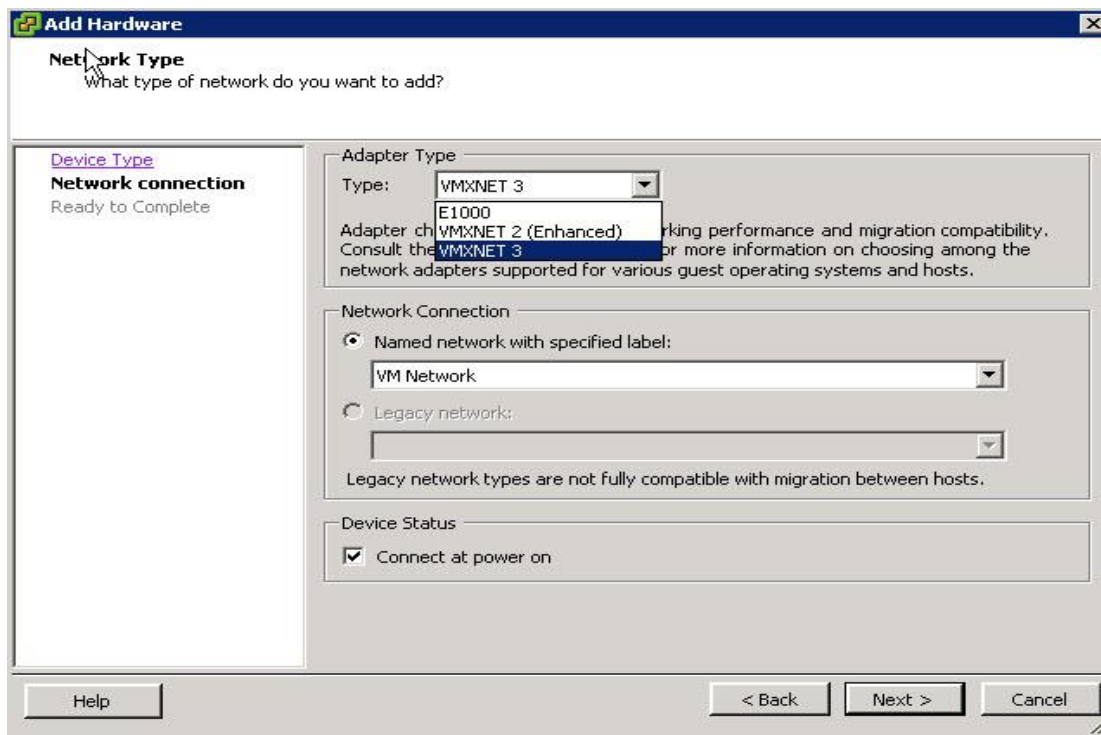




3. Click **Add** to go to the **Add Hardware** window.

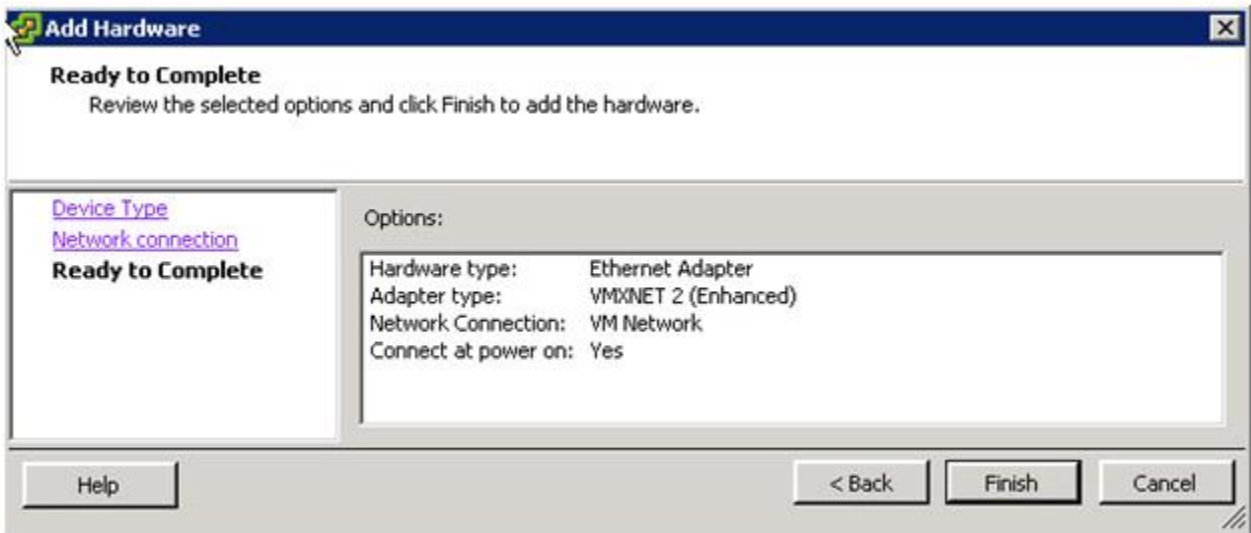


4. Select the **Device Type** and click **Next >**.

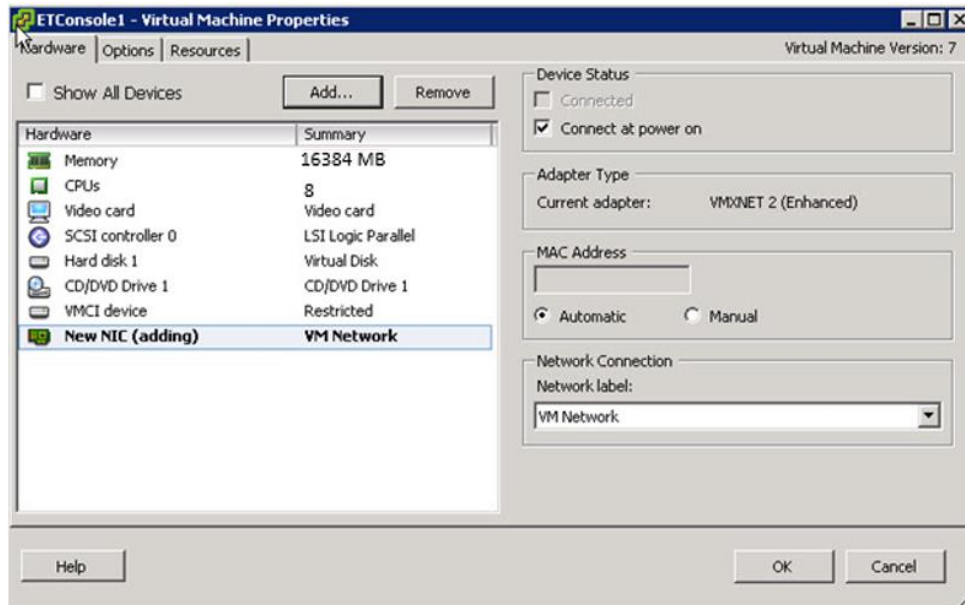


5. In the **Adapter Type** pane, select **Type:** drop-down, and select **VMXNET 2 (Enhanced)** or **VMXNET 3**.

- Click **Next** and the **Ready to Complete** page opens.



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



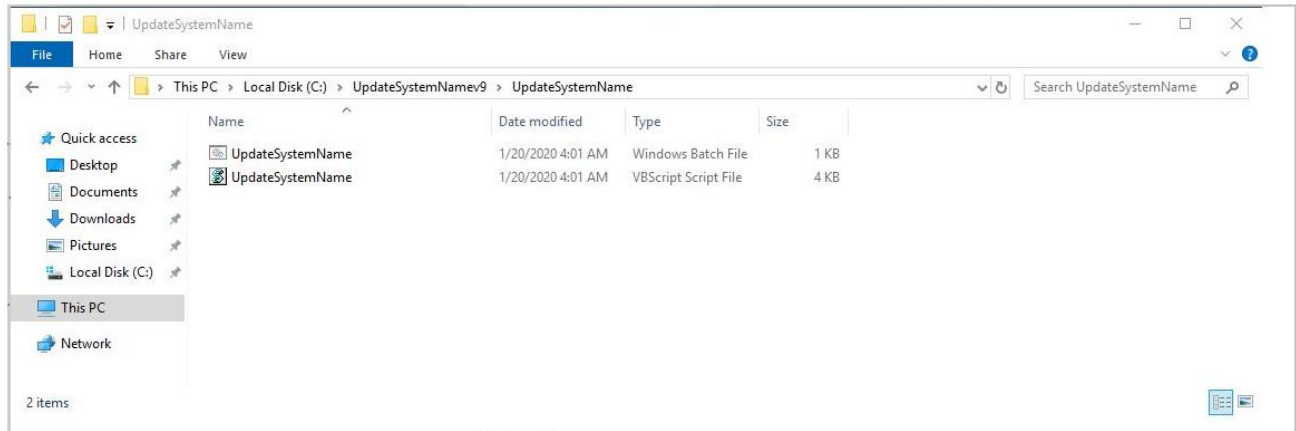
## 1.7 Configuring EventTracker Virtual Appliance

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#

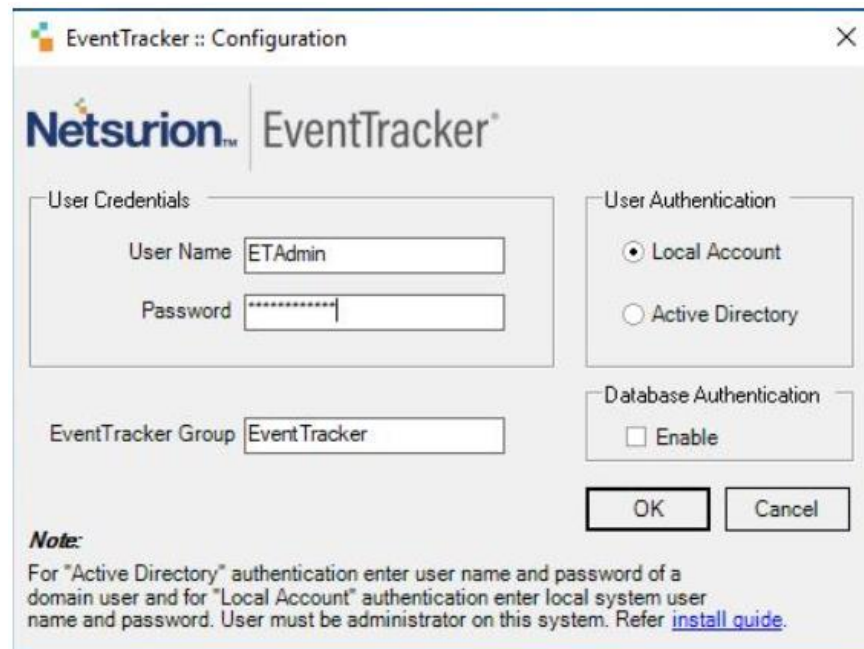
**NOTE:** On the first successful logon you will be prompted to change the ETAdmin user password. Change it to secure password and keep it safe.

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 [Update System Name](#) 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**.

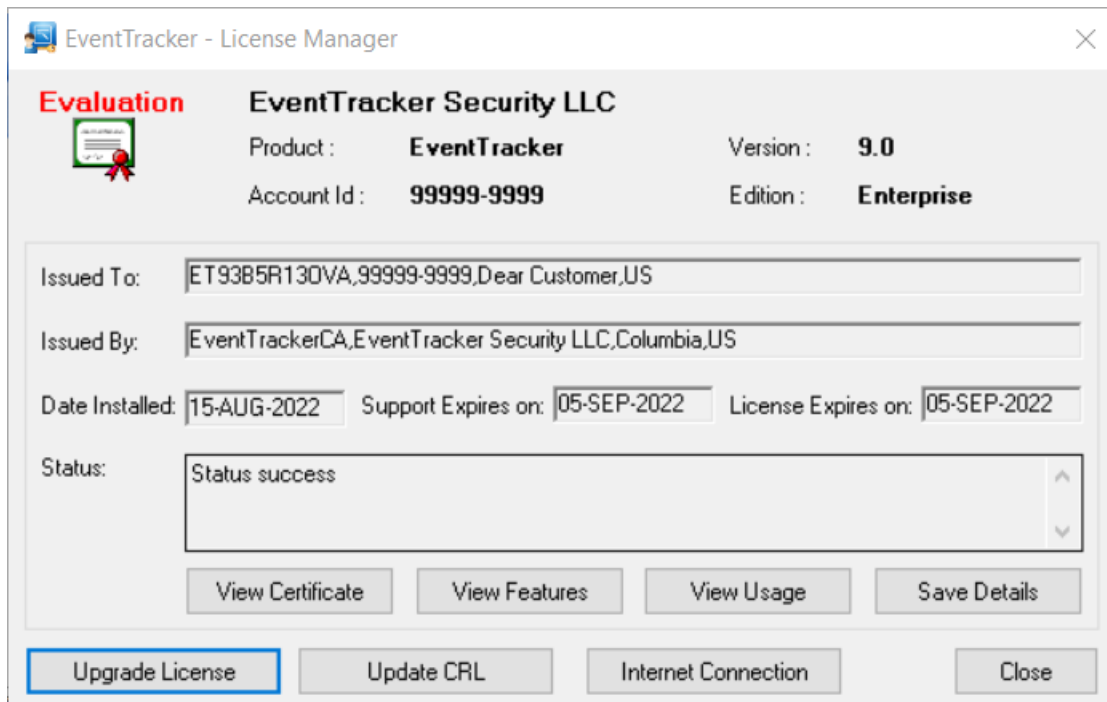


7. Update the user credential ETAdmin user or select an active directory and enter domain user credentials.
8. After **EventTracker Configuration** validates the credential and runs successfully, install **VMware Tools** on newly imported Virtual machine.
9. Change **startup type** to **Automatic** for 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**.

11. The **EventTracker Control Panel** window displays.






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



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 <a href="#">View all</a>
State:	Powered On
Active Tasks:	
vSphere HA Protection:	 N/A 

## 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 [www.netsurion.com](http://www.netsurion.com).

## 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>