

# ExtremeAnalytics Virtual Sensor 1.0.0 Software Installation Guide

## Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks)

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: [www.extremenetworks.com/support/policies/software-licensing](http://www.extremenetworks.com/support/policies/software-licensing)

# Contents

---

- Preface..... 5**
  - Conventions..... 5
    - Notes, cautions, and warnings..... 5
    - Text formatting conventions..... 5
    - Command syntax conventions..... 6
  - Documentation and Training..... 6
  - Getting Help..... 6
    - Subscribing to Service Notifications..... 7
  - Providing Feedback to Us..... 7
- Getting Started..... 9**
  - System requirements..... 9
  - Downloading the distribution..... 9
- Virtual Sensor installation..... 11**
  - Prerequisites..... 11
  - Virtual Sensor installation using XMC and XMC Connect..... 14
  - Virtual Sensor installation using vSphere Web Client..... 15
    - Deployment architecture..... 15
    - Installing Virtual Sensor using vSphere Web Client..... 16
- Post-installation configuration..... 29**
- Troubleshooting..... 31**



# Preface

- Conventions..... 5
- Documentation and Training..... 6
- Getting Help..... 6
- Providing Feedback to Us..... 7

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

## Conventions


This section discusses the conventions used in this guide.


### Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

**NOTE**  
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

**ATTENTION**  
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

 **CAUTION**  
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

 **DANGER**  
*A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.*

### Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
<b>bold text</b>	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
<i>italic text</i>	Identifies emphasis.
	Identifies variables.
	Identifies document titles.

Format	Description
Courier font	Identifies CLI output.
	Identifies command syntax examples.

## Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ x   y   z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x   y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

## Documentation and Training

Find Extreme Networks product information at the following locations:

- [Current Product Documentation](#)
- [Archived Documentation](#) (for earlier versions and legacy products)
- [Release Notes](#)
- [Hardware/software compatibility matrices](#) for Campus and Edge products
- [Supported transceivers and cables](#) for Data Center products
- [Other resources](#), like white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

## Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- Extreme Portal** Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- The Hub** A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

**Call GTAC**

For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

## Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to [www.extremenetworks.com/support/service-notification-form](http://www.extremenetworks.com/support/service-notification-form).
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

### NOTE

You can modify your product selections or unsubscribe at any time.

4. Click **Submit**.

## Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at [documentation@extremenetworks.com](mailto:documentation@extremenetworks.com).

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.





# Getting Started

- [System requirements](#)..... 9
- [Downloading the distribution](#)..... 9

ExtremeAnalytics Virtual Sensor enables data center operators to get deep application-level visibility and performance measurements for VM-to-VM traffic within a host or across hosts. For security use cases, Virtual Sensor enables smart packet captures and unsampled IPFIX for IPv4 and IPv6 traffic.

Virtual Sensor can run on a VM with VMware ESXi as hypervisor host managed by vCenter.

## System requirements

The table below shows the system requirements for Virtual Sensor OVA image:

TABLE 1 System requirements

Entity	VS100 - Small deployment	VS250 - Medium deployment
vCPU	1	2
RAM	512 MB	2 GB
vNIC	5	5
HDD	16 GB	16 GB
Driver	VMXNET3	VMXNET3
Hypervisor	VMware ESXi 6.0/6.5/6.7	VMware ESXi 6.0/6.5/6.7
OS	<b>Release version:</b> CentOS release 7.2 x86_64 x86_64 x86_64 GNU/Linux  <b>Kernel version:</b> 3.10.0-327.el7.x86_64	<b>Release version:</b> CentOS release 7.2 x86_64 x86_64 x86_64 GNU/Linux  <b>Kernel version:</b> 3.10.0-327.el7.x86_64

## Downloading the distribution

Perform the following steps to download the distribution for Virtual Sensor 1.0.0 from the Extreme Networks website:

1. Go to the [Extreme Portal](#) website and log in with your username and password.
2. If you are visiting Extreme Portal for the first time, click **Register Now** instead and follow the prompts to register. You may need to enter the access code/serial number you received in your order confirmation e-mail to view and download all files.
3. On the main page, click **Products** and then click **ExtremeAnalytics**.
4. On the **ExtremeAnalytics** page, click **ExtremeAnalytics Virtual Sensor**. A list of products is displayed.
5. Go to:
  - **Software / Release Notes** -> **Software & Downloads** -> **1.0.0** for Virtual Sensor installation files.
  - **Software / Release Notes** -> **Release Notes** for Virtual Sensor Release Notes.
  - **Documentation** -> **1.0.0** for Virtual Sensor documentation.
6. Click a file to download.

7. Save the file to a local directory on your system.

# Virtual Sensor installation

• Prerequisites.....	11
• Virtual Sensor installation using XMC and XMC Connect.....	14
• Virtual Sensor installation using vSphere Web Client.....	15

This chapter provides information about installing the ExtremeAnalytics Virtual Sensor.

Virtual Sensor can be installed using one of the following methods:

- **Method 1 - XMC Connect:** See the section [ExtremeAnalytics Virtual Sensor Configuration](#) in *ExtremeAnalytics User Guide*
- **Method 2 - vSphere Web client:** See the section [Virtual Sensor installation using vSphere Web Client](#) on page 15

When Virtual Sensor is installed, it is provisioned and added to the device list in XMC using built-in Enhanced Zero Touch Provisioning (ZTP+), which is a method for devices to communicate with XMC. ZTP+ allows a device to obtain firmware and configuration updates from XMC, and publish status, statistics and device events to XMC.

During installation, Virtual Sensor automatically starts the Linux process `cloud-connector client`. The cloud-connector client relies on the Default VLAN 1 enabled DHCP client to discover a DHCP server.

After Virtual Sensor receives an IP address and a Domain Name from the DHCP server, it begins the DNS query to find the built-in Extreme Networks Management Appliance Fully-Qualified Domain Name (FQDN) `extremecontrol@<domain-name>` for Extreme Management Center. `<domain-name>` is the domain assigned by the DHCP server.

The cloud-connector tries to resolve these names in an endless round-robin loop. When any of the names are resolved to an IP address, Virtual Sensor attempts connection to that IP address.

After the Virtual Sensor installation is complete, Cloud Connector saves the configuration on the device and terminates.

## Prerequisites

Before deploying Virtual Sensor, ensure that the following are available and configured:

- **Extreme Management Center (XMC) 8.4**
  - Configure SNMP and CLI credentials for Virtual Sensor in XMC. It is required to use SNMPv3 and the CLI credentials, and cannot have a blank password. For more information, see the section [Profiles](#) in *ExtremeAnalytics User Guide*.

- **Hypervisor:** VMware vSphere-based data center with vCenter managed ESXi

Virtual Sensor is packaged in the OVA file format (defined by VMware), and it must be deployed on a VMware ESXi hypervisor.

- **vCenter privileges and permissions**

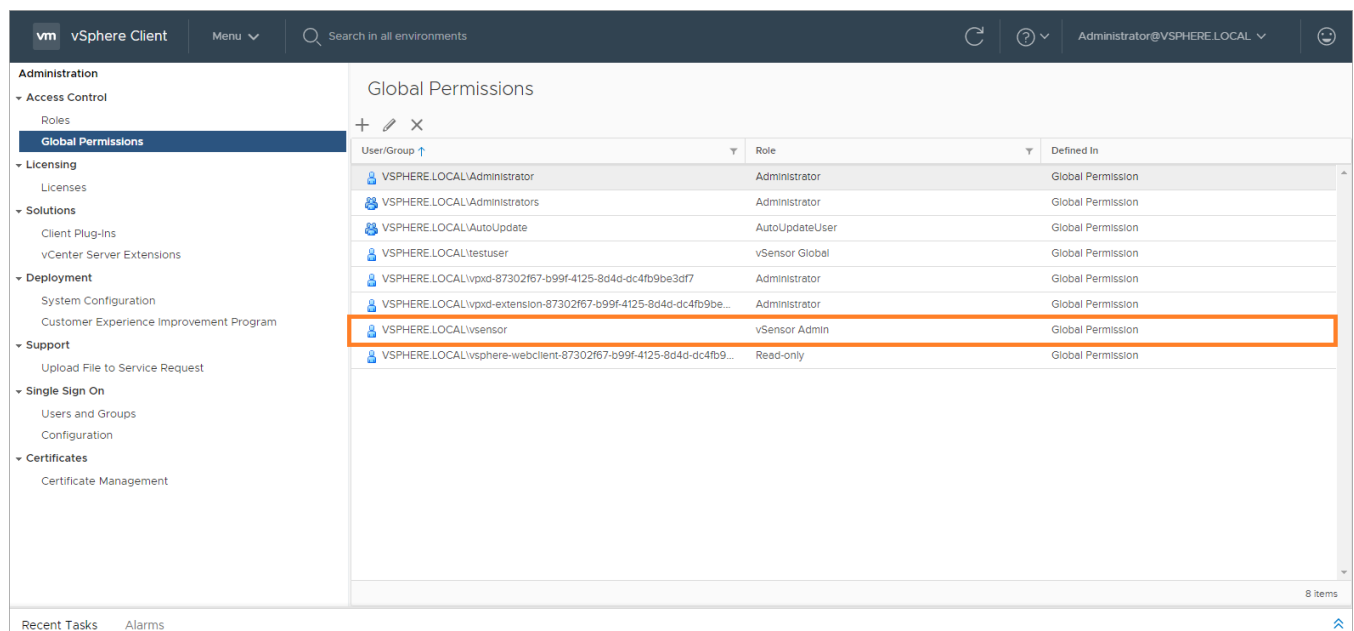
Configure vCenter vSphere login with an administrative role with the following Global Permissions:

**TABLE 2** vCenter Global Permissions

Privilege name	Permissions
Distributed Switch <ul style="list-style-type: none"><li>– VSPAN operation</li></ul>	All
Datastore <ul style="list-style-type: none"><li>– Allocate space</li><li>– Browse datastore</li></ul>	All

TABLE 2 vCenter Global Permissions (continued)

Privilege name	Permissions
Host	All
<ul style="list-style-type: none"> <li>Local operations <ul style="list-style-type: none"> <li>Create virtual machine</li> <li>Delete virtual machine</li> <li>Reconfigure virtual machine</li> </ul> </li> </ul>	
Network	All
<ul style="list-style-type: none"> <li>Assign network</li> </ul>	
vAPP	All
<ul style="list-style-type: none"> <li>Import</li> <li>View OVF environment</li> </ul>	



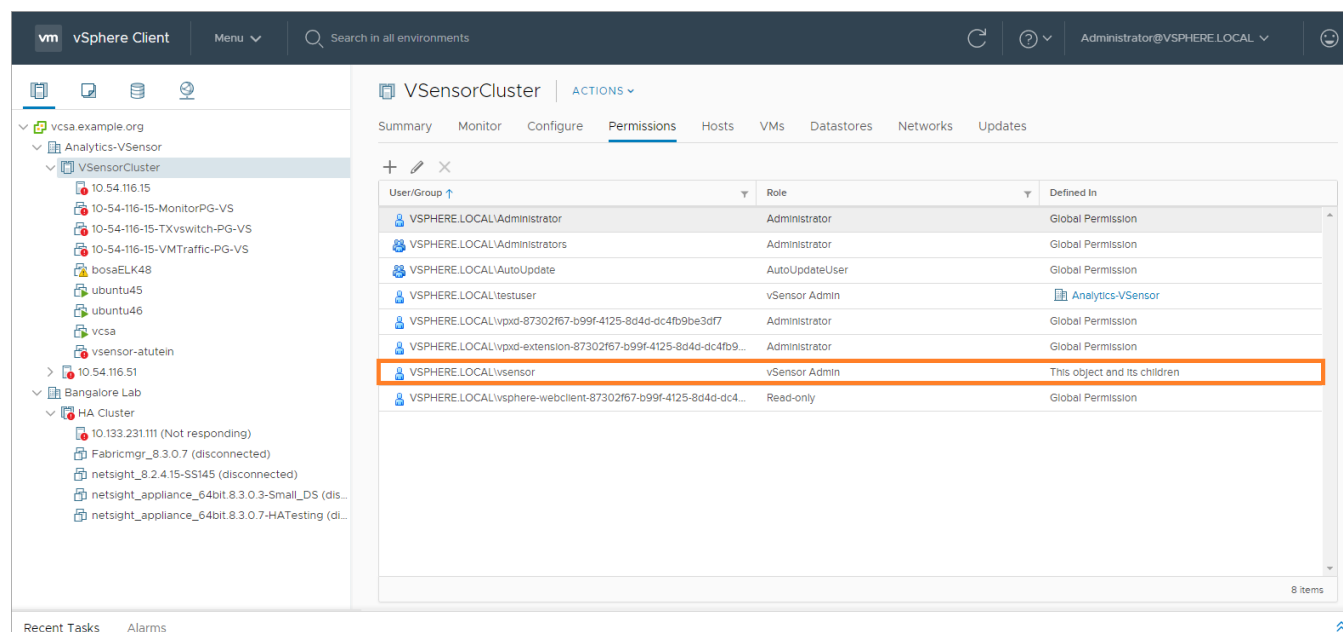
Configure vCenter vSphere login with an administrative role with the following permissions in the cluster the Virtual Sensor is monitoring:

TABLE 3 vCenter Global Permissions

Privilege name	Permissions
Distributed Switch	All
<ul style="list-style-type: none"> <li>VSPAN operation</li> </ul>	
Datastore	All
<ul style="list-style-type: none"> <li>Allocate space</li> <li>Browse datastore</li> <li>Remove file</li> </ul>	
Host	All
<ul style="list-style-type: none"> <li>Local operations <ul style="list-style-type: none"> <li>Create virtual machine</li> <li>Delete virtual machine</li> <li>Reconfigure virtual machine</li> </ul> </li> </ul>	

TABLE 3 vCenter Global Permissions (continued)

Privilege name	Permissions
Network	All
– Assign network	
Tasks	All
– Create task	
– Update task	
vAPP	All
– Import	
– View OVF environment	
Virtual machine	All
– Change Configuration	
> Add new disk	
> Advanced configuration	
– Edit Inventory	
> Create new	
> Remove	
– Interaction	
> Power off	
> Power on	



- **DHCP and DNS servers (required for ZTP+)**

Configure the DHCP and DNS servers on your network for discovery of the new Virtual Sensor deployment.

For Virtual Sensor to communicate with XMC:

- The DHCP Server (that will be serving an IP to Virtual Sensor) needs to return a DNS Server and Domain Name to Virtual Sensor.
- The DNS Server needs to map the name `extremecontrol.<domain-name>` to the IP address of the Extreme Management Center server.
- Confirm that the DHCP server is serving the correct DNS and domain name information.

**NOTE**

For full instructions on configuring DHCP, NPS, and DNS services, refer to *ExtremeCloud Appliance Deployment Guide* located in the Extreme Networks documentation portal: <https://extremenetworks.com/documentation/extremecloud-appliance>.

## Virtual Sensor installation using XMC and XMC Connect

Virtual Sensor can be installed using XMC and XMC Connect. We recommend installing the Virtual Sensor using this method unless you do not have the required permissions from your VMware Administrator. When installing the Virtual Sensor using the vSphere client, some information does not populate on the Analytics > Configuration > Virtual Sensors tab in Extreme Management Center, including the **Physical Host**, **Monitored Switch**, **Port Group**, and **VMs Monitored** fields in the Virtual Sensors table at the top of the tab and the Virtual Machines table at the bottom of the tab.

For more information about installing Virtual Sensor using XMC and XMC Connect, see the section [ExtremeAnalytics Virtual Sensor Configuration](#) in *ExtremeAnalytics User Guide*.

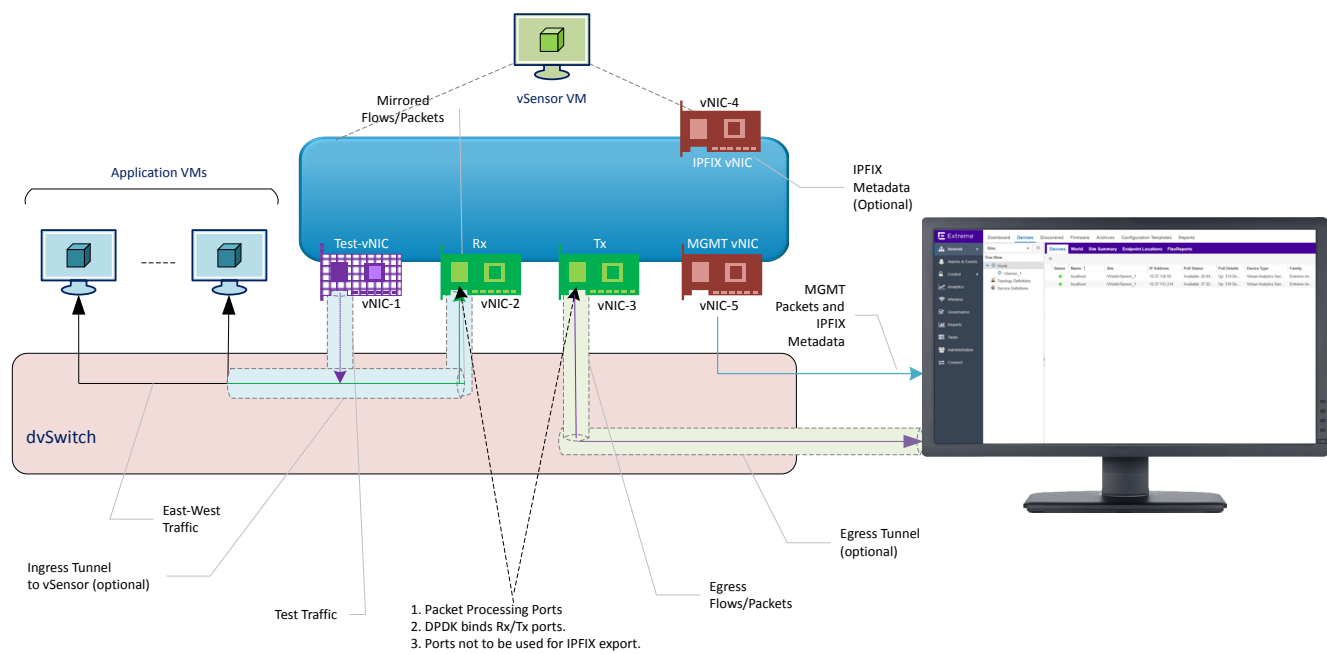
## Virtual Sensor installation using vSphere Web Client

This section provides information about the Virtual Sensor deployment architecture and steps for installing Virtual Sensor using vSphere Web Client.

## Deployment architecture

The image below shows a typical Virtual Sensor deployment on a VMware ESXi hypervisor:

**FIGURE 1** Deployment architecture



Virtual Sensor is based on CentOS 7.2 and DPDK, and deployed using VMware vSphere-based OVA image.

The Virtual Sensor OVA image is preconfigured with five vNICs: Rx (for receiving ingress packets), Tx (for sending packets post-processing), Test (for sending test packets), IPFIX Export (for exporting IPFIX metadata), and Management.

- The Rx vNIC and Test vNIC should be in a port group on the dvSwitch you wish to monitor.
- The Tx vNIC, Management vNIC, and IPFIX vNIC should be in the same network. This must be a network that can access the XMC and Analytics appliances.
- To monitor traffic from multiple switches, one instance of Virtual Sensor must be deployed per switch, since the Rx vNIC cannot be part of multiple switches at the same time.
- When added as a flow source to an ExtremeAnalytics engine, Virtual Sensor forwards the first few packets of each flow over a GRE tunnel to the ExtremeAnalytics engine and sends flow metadata in the form of IPFIX records to the engine over the network.

- Virtual Sensor supports metadata export in IPFIX format based on the configuration.

## Installing Virtual Sensor using vSphere Web Client

### NOTE

Ensure that all the prerequisites are met, as outlined in the section [Prerequisites](#) on page 11.

Perform the following steps to install Virtual Sensor using vSphere Web Client on a vCenter-managed ESXi:

1. Download the Virtual Sensor OVA image to your local machine where the vSphere client is installed and running.

### NOTE

For information about downloading the OVA image, see the section [Downloading the distribution](#) on page 9.

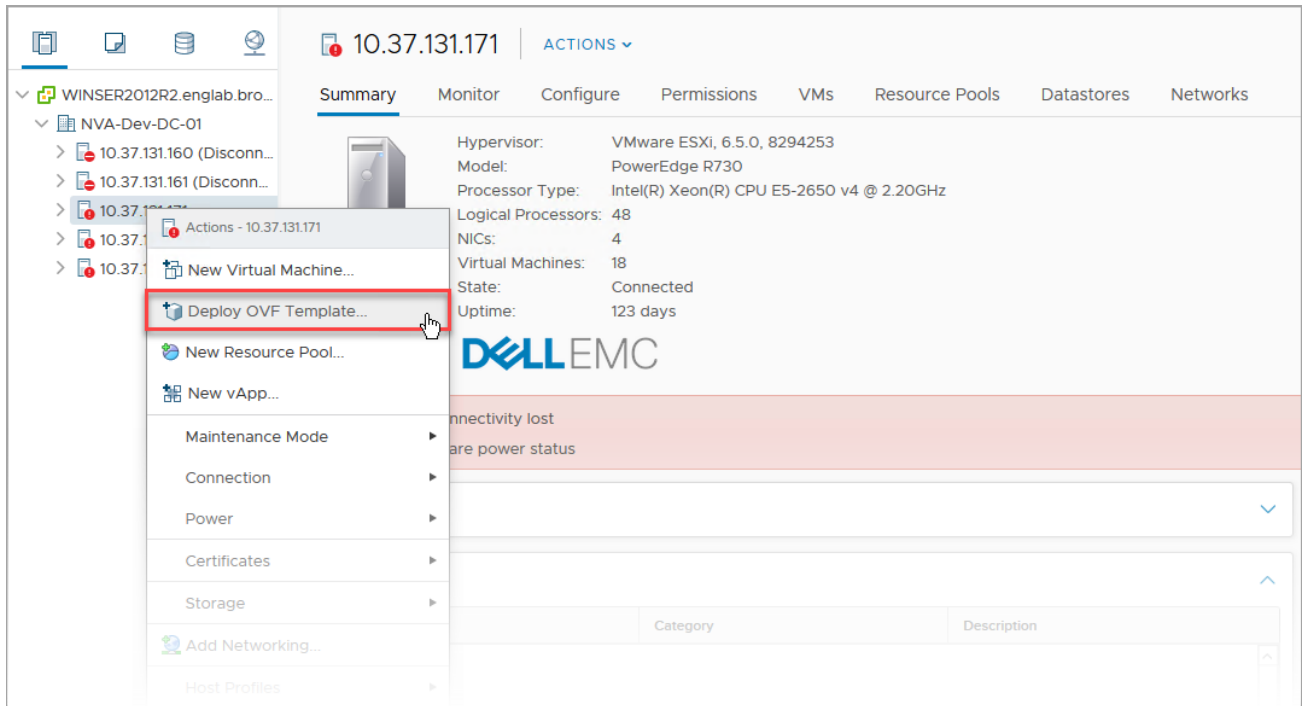
2. Launch a Web browser window and enter the URL for the vSphere Web client.
3. Enter your username and password, and click **Log In**.



#### 4. Install OVA image

- a) On the Navigator pane, right-click the ESXi on which you want to install Virtual Sensor OVA image and click **Deploy OVF Template**.

FIGURE 2 Deploy OVF Template



**Deploy OVF Template** window appears.

- b) Click **Browse** to browse to select the Virtual Sensor OVA image you downloaded in [Step 1](#) and click **Open**.

FIGURE 3 OVA image

**Deploy OVF Template**

**1 Select an OVF template**

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

**Select an OVF template**

Select an OVF template from remote URL or local file system

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.

☐ URL

☒ Local file

vsensor-1.0-sqa\_31\_small.ova

- c) Enter a name and the location for your virtual machine.
- d) Select the destination compute resource.
- e) Review the details for the selection so far and click **Next**.
- f) Click **Next**.  
The **Select storage** page appears.
- g) Click a datastore from the list of accessible datastores and click **Next**.  
The **Select networks** page appears.
- h) The **Select Networks** page is used to map the Virtual Sensor port to the virtual network deployed on the ESXi host.  
Select the network or port group for each virtual network adapter:
  - **EgressNetwork**, **MgmtNetwork**, and **FlowExportNetwork** must be on the management network and able to reach the XMC and Analytics engine
  - **TestIntfNetwork** and **IngressNetwork** must be on a port group on the dvSwitch you want to monitor

FIGURE 4 Select networks

**Deploy OVF Template**

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**
- 7 Customize template
- 8 Ready to complete

**Select networks**  
Select a destination network for each source network.

Source Network	Destination Network
EgressNetwork	VM Network
MgmtNetwork	VM Network
TestIntfNetwork	pg1
FlowExportNetwork	VM Network
IngressNetwork	pg1

5 items

**IP Allocation Settings**

IP allocation: Static - Manual

IP protocol: IPv4

[CANCEL](#) [BACK](#) [NEXT](#)

TABLE 6 Select networks

Source Network	Destination Network
EgressNetwork	For sending packets post-processing. Select your management network as the Destination Network.
MgmtNetwork	Select your management network as the Destination Network.
TestIntfNetwork	For sending a test pcap to the Rx interface.
FlowExportNetwork	For exporting IPFIX metadata. Select your management network as the Destination Network.
IngressNetwork	For receiving ingress packets.

- i) Click **Next**.  
The **Customize template** page appears.  
Enter appropriate values for the following properties:

TABLE 7 Customize template

Property	Description
Host Network IP Address	This the management IP address. If this IP address is not provided, it is assigned by the DHCP server.
Host Network Prefix	Prefix length, which is the number of bits set in the subnet mask. For example: If the subnet mask is 255.255.255.0, the prefix length is 24 bits.
Host Network Default Gateway	This is the default gateway.
Host Name	Hostname for the VM.

**TABLE 7** Customize template (continued)

Property	Description
	<p>The length of the hostname can be up to 64 characters. It can contain alphanumeric characters and hyphens.</p> <p><b>NOTE</b> Hostname cannot start or end with a hyphen.</p>
Domain Name	
DNS IP Address	This is the DNS server IP address. This is mandatory.
NTP IP Address	NTP server IP address.
NTP Timezone	<p>Network Time Protocol (NTP) time zone. For example, <i>America/New_York</i>. Run the following Linux command to list the available time zones:</p> <pre>timedatectl list-timezones</pre>
XMC IP Address	XMC IP address. This is optional. If this IP address is not provided, it is assigned by the DHCP server.
Root password	<p>This is the password for the root user on the ESXi host on which Virtual Sensor is being deployed.</p> <p><b>NOTE</b> If CLI credentials for Virtual Sensor are already configured in XMC, those credentials take precedence over the password set here. For information about setting the CLI credentials in XMC see the section, <a href="#">CLI Credentials</a> in <i>ExtremeAnalytics User Guide</i>.</p>

FIGURE 5 Customize template

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Customize template**
- 8 Ready to complete

### Customize template

Customize the deployment properties of this software solution.

✓ All properties have valid values

Application	10 settings
Host Network IP Address	Network address 10.37.138.181
Host Network Prefix	Network prefix length.Range 0-32 20
Host Network Default Gateway	IP address of default gateway. 10.37.128.1
Host Name	The hostname length cannot be greater than 64 characters, and it can contain only alphanumeric characters and hyphens. Hyphen cannot be used at the beginning and at the end. vsVM1
Domain Name	Domain name. nameserver
DNS IP Address	DNS IP address. 10/37.2.1
NTP IP Address	NTP IP address. 10.37.2.74
NTP Timezone	NTP Timezone. America/New_York
XMC IP Address	XMC IP address. 10.37.138.138
Root password	Root password password123

CANCEL
BACK
NEXT

- j) Click **Next**.  
The **Ready to complete** page appears.
- k) On the **Ready to complete** page, review the configuration settings for the virtual machine.
- l) Click **Finish**.  
The virtual machine appears in the inventory.
- m) After the VM has powered on, log on to the Virtual Sensor VM with the following credentials:
  - **localhost login:** root
  - **Password:** password

If you have provided the XMC IP address, Virtual Sensor tries to connect to XMC using ZTP+. Otherwise, Virtual Sensor tries to resolve the extremecontrol host name to IP using DNS.

This completes Virtual Sensor installation on a single ESXi host. Repeat the steps above for installing Virtual Sensor on additional ESXi hosts.

Complete the remaining steps in XMC to discover and add the device to the inventory. For more information, see the section [Post-installation configuration](#) on page 29.

#### NOTE

If Virtual Sensor receives traffic as it is initializing, packet drops (reported as mbuf allocation failure) may be observed.

## Recommended vCenter settings for Virtual Sensor

The following vCenter settings are recommended for optimal performance of your Virtual Sensor VM:

1. Power off the Virtual Sensor VM.
2. Right-click the VM and select **Edit Settings**.
3. On the **Virtual Hardware** tab, expand **CPU**, and allocate the CPU capacity as follows:

TABLE 8

Option	Description
Reservation	Reservation = number of vCPUs * CPU speed of ESXi <b>Example</b> <ul style="list-style-type: none"> <li>• Medium OVA: 2 * 2297 = 4594 MHz</li> <li>• Small OVA: 1 * 2297 = 2297 MHz</li> </ul>
Shares	Set this to <b>High</b> .

4. Click **OK**.
5. Right-click the Virtual Sensor VM again and select **Compatibility > Upgrade VM Compatibility**.  
The virtual hardware is upgraded to the latest supported version.

#### NOTE

The **Upgrade VM Compatibility** option only appears if the virtual hardware on the VM is not the latest supported version.

6. Click **Yes** to continue with the upgrade.
7. Power on the virtual machine.

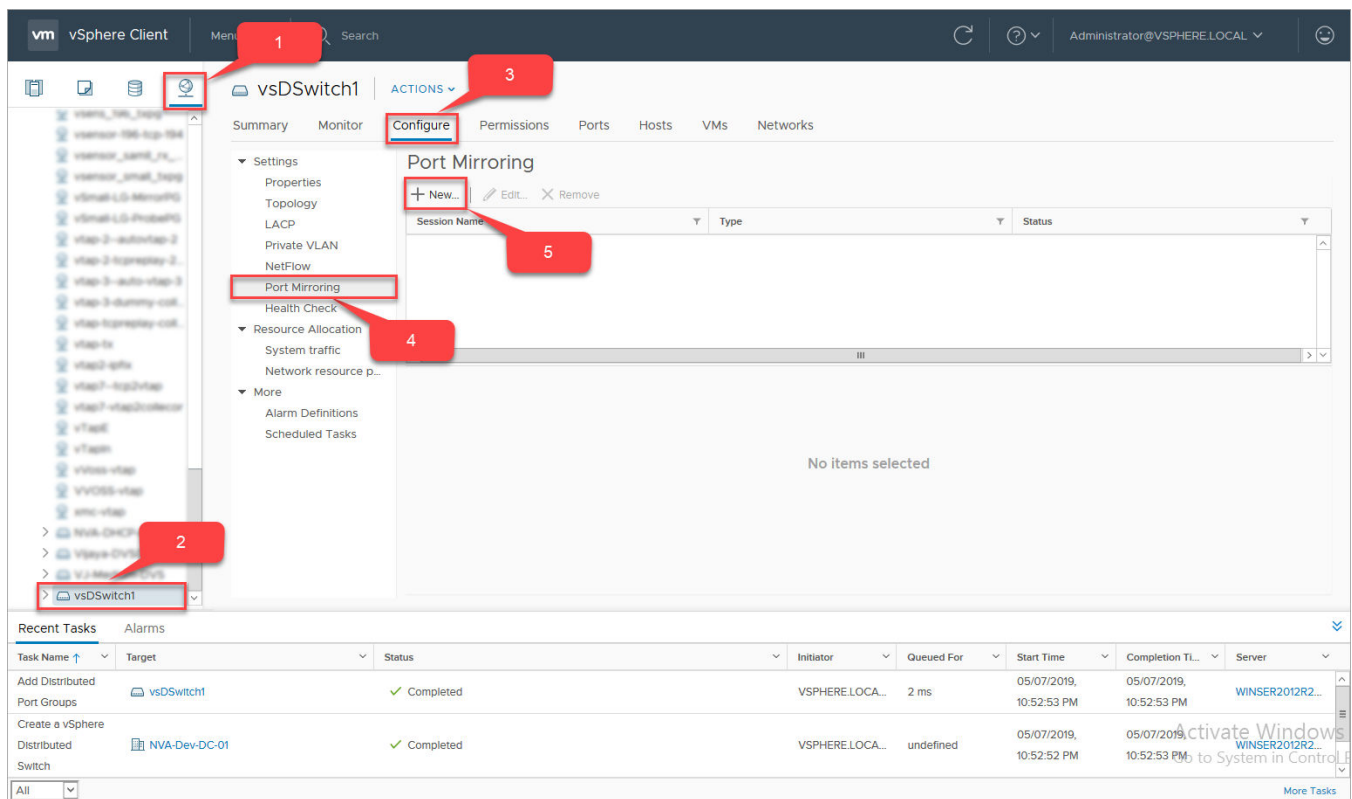
## Creating a Port Mirroring session to monitor traffic

Port mirror configuration is done at the Distributed Switch level. A port mirror session is created by identifying the traffic source that needs to be monitored and the traffic destination where the traffic will be mirrored to. The traffic source can be any port with ingress, egress or all traffic selected. The traffic destination can be any virtual machine or vmknic. After a port mirror session is configured, the Distributed Switch copies packets to the destination.

Perform the following steps to create a port mirroring session:

1. Log in to the vSphere Client and:
  - a) Click the **Networking** tab.
  - b) Click the Distributed Switch you want to configure. `vsDSwitch1` is used in this example.
  - c) Click the **Configure** tab and then click **Port Mirroring**.

FIGURE 6 Port Mirroring



2. Click **New**.

**Add Port Mirroring Session** window appears.

Ensure that **Distributed Port Mirroring** is selected.

**FIGURE 7** Add Port Mirroring Session

vsDSwitch1 - Add Port Mirroring Session

**1 Select session type**  
**2 Edit properties**  
**3 Select sources**  
**4 Select destinations**  
**5 Ready to complete**

Select session type  
Select the type of the port mirroring session.

☒ **Distributed Port Mirroring**  
☐ Remote Mirroring Source  
☐ Remote Mirroring Destination  
☐ Encapsulated Remote Mirroring (L3) Source

Descriptions per session type ⓘ

CANCEL BACK NEXT

Click **Next**.



3. In the **Edit properties** section:
  - Enter a meaningful name in the **Name** field
  - Change **Status** to **Enabled**.

Leave all the other fields unchanged.

**FIGURE 8** Edit properties

vsDSwitch1 - Add Port Mirroring Session

✓ 1 Select session type  
**2 Edit properties**  
3 Select sources  
4 Select destinations  
5 Ready to complete

**Edit properties**  
Specify a name and the properties of the port mirroring session.

Name vSensorTap1

Status **Enabled** ▼

Session type Distributed Port Mirroring

**Advanced properties**

Normal I/O on destination ports Disallowed ▼

Mirrored packet length ☐ Enable 60

Sampling rate 1

Description

CANCEL BACK NEXT

Click **Next**.

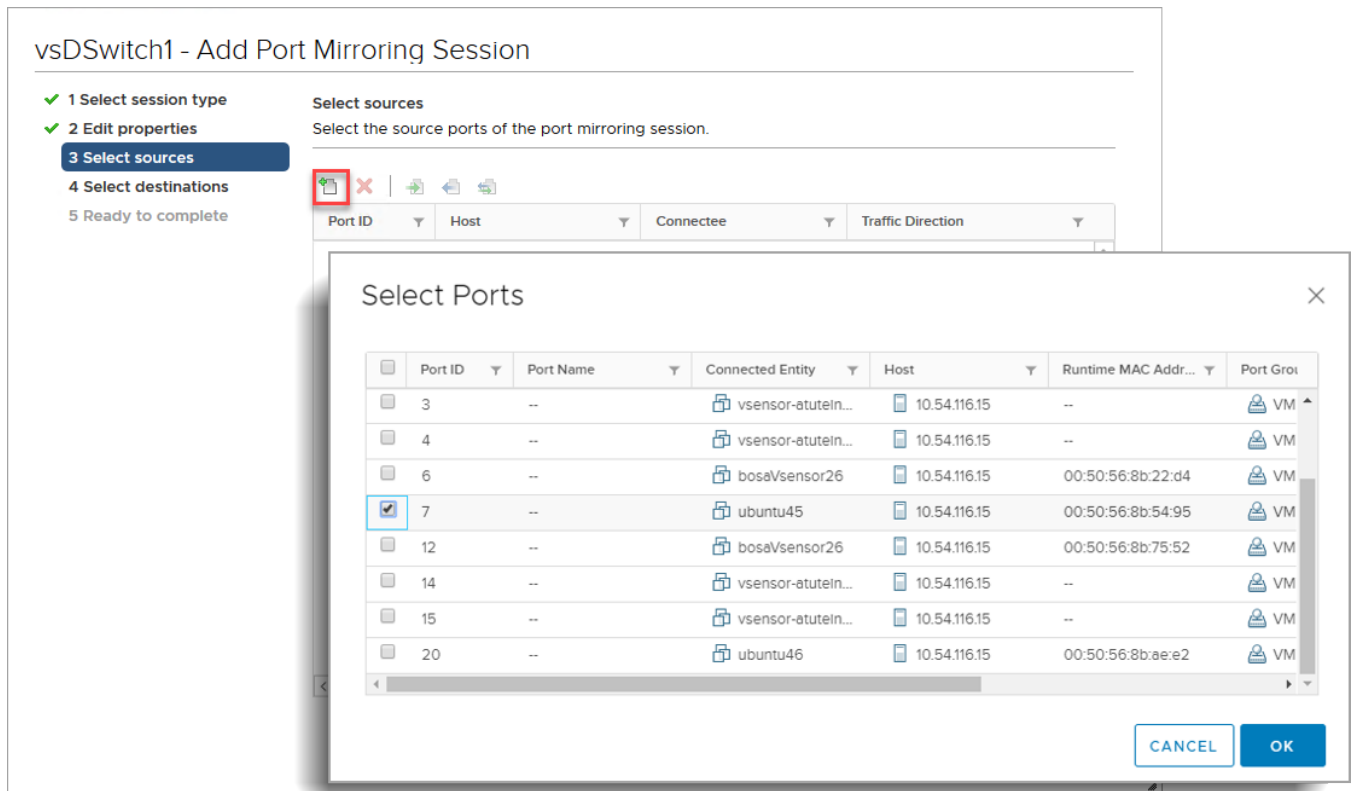
4. In the **Select sources** section, click the **Add** icon to select ports to be monitored.

**Select Ports** window appears.

Select the relevant ports and click **OK**.

Optionally, change the mirror to either Ingress or Egress, or leave it as Ingress/Egress.

**FIGURE 9** Select Ports



The selected ports appear in the list.

FIGURE 10 Select source ports

vsDSwitch1 - Add Port Mirroring Session

✓ 1 Select session type  
✓ 2 Edit properties  
**3 Select sources**  
4 Select destinations  
5 Ready to complete

Select sources  
Select the source ports of the port mirroring session.

✚ ✖ | ✚ ⬅ ➡ ✚

Port ID	Host	Source	Traffic Direction
7	10.54.116.15	ubuntu45	Ingress/Egress

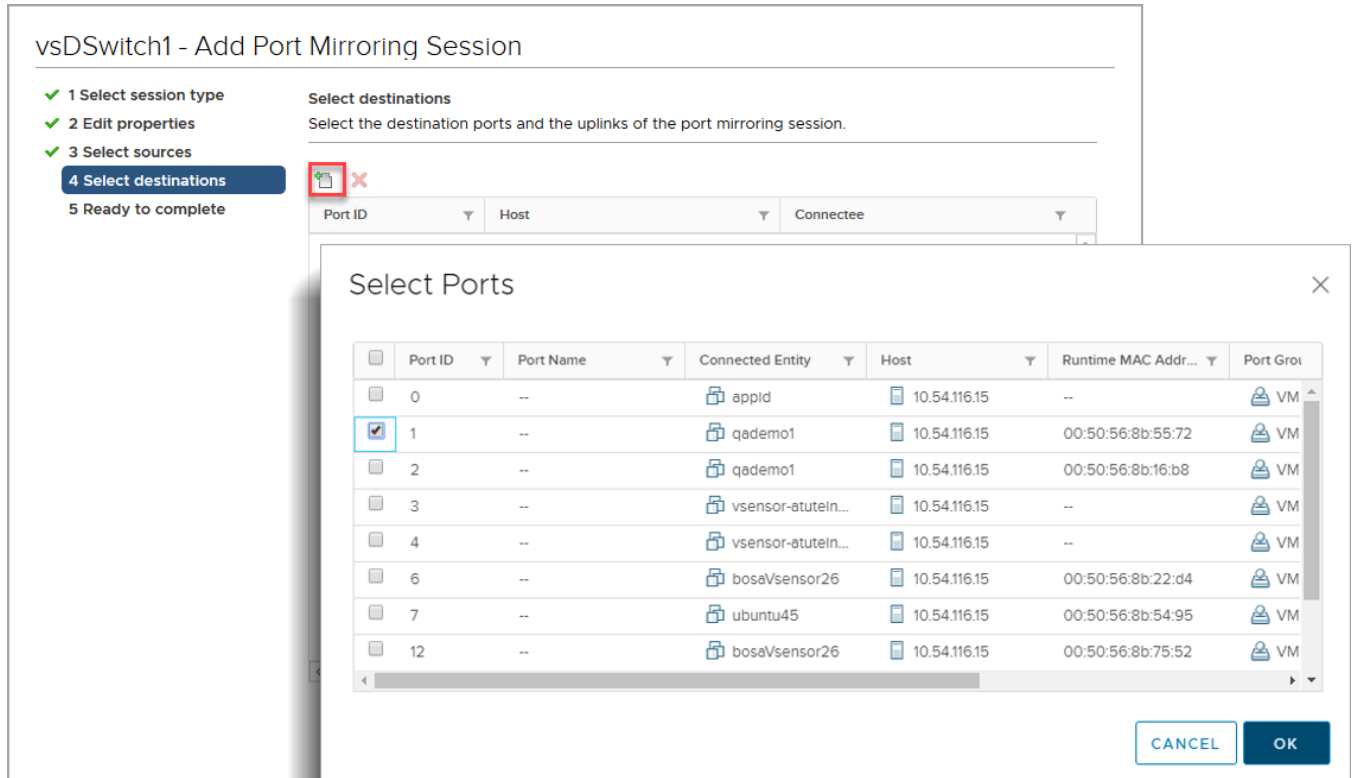
Mirror all ingress and egress packets by the port.

CANCEL BACK NEXT

Click **Next**.

5. In the **Select destinations** section, click the **Add** icon to select a destination port. Select the ingress interface of the Virtual Sensor. Make sure to match the MAC address, as the testintf interface will also be in the same port group.

FIGURE 11 Select destination ports



6. Click **Finish**.

# Post-installation configuration

---

This chapter provides information about the steps to be performed in XMC to discover and display the device.

Perform the following steps:

1. Login to XMC and verify that the Virtual Sensor device is displayed in the [Discovered](#) tab.
2. Right-click the device and click **Configure Devices**.
  - a) In the **Device** tab, set the Administration Profile. For more information, see the section [Device](#).
  - b) Click the **ZTP+ Device Settings** tab to configure the ZTP+ settings. For more information, see the section [ZTP+ Device Settings](#).
3. Click **Save**. The **Status** column changes to ZTP+ Staged.

After a few minutes, the device appears in the **Devices** tab. For more information, see the section [Devices](#).



# Troubleshooting

---

This chapter provides guidelines for diagnosing and troubleshooting issues with ExtremeAnalytics Virtual Sensor installation.

## Cloud-connector process in loop

If the cloud-connector process fails to resolve the IP address and is stuck in an endless loop, perform the following steps:

1. Login to the Virtual Sensor VM and check the cloud-connector log file, located at `/tmp/cloud.log`.
2. Try to install Virtual Sensor again using one of the following methods:
  - **XMC Connect:** See the section [ExtremeAnalytics Virtual Sensor Configuration](#) in *ExtremeAnalytics User Guide*
  - **vSphere Web client:** See the section [Virtual Sensor installation using vSphere Web Client](#) on page 15