ExtremeAnalytics Virtual Sensor 1.0.0

Software Installation Guide

Table of Contents

Preface

Read the following topics to learn about:

* The meanings of text formats used in this document.
* Where you can find additional information and help.
* How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
[ ]	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, such as passwords, are enclosed in angle brackets.
…	Repeat the previous element, for example, `member[member...]`.
\	In command examples, the backslash indicates a "soft" line break. When 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

Release Notes

Hardware and software compatibility for Extreme Networks products

Extreme Optics Compatibility

Other resources such as 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/.

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: (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

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions 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

Subscribe to Product Announcements

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

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

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

Providing Feedback

The Information Development team at Extreme Networks has 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 we especially want to know about:

- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

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

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.

> **Note**
> ExtremeAnalytics Virtual Sensor is not available for sale and instructions are intended for existing customers only. Support will be depreciated after the ExtremeCloud IQ - Site Engine version 21.9 release.

System requirements

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

Table 4: 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	**Release version**: CentOS release 7.2 x86_64 x86_64 x86_64 GNU/Linux **Kernel version**: 3.10.0-327.el7.x86_64	**Release version**: CentOS release 7.2 x86_64 x86_64 x86_64 GNU/Linux **Kernel version**: 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, select **Products** and then select **ExtremeAnalytics**.

4. On the **ExtremeAnalytics** page, select **ExtremeAnalytics**.

   A list of products is displayed.

5. On the **Software/Release Notes** tab, select the **Advance Page** button until **8.3.0.111.Analytics** displays.

6. Select **8.3.0.111.Analytics** to view the files available for download.

7. Select **VirtualSensor Small OVA** or **VirtualSensor Medium OVA**, depending on your configuration.

   The **File Details** window displays.

8. Select the **Download File** button.

   The **Confirm Customer Information** window displays.

9. Verify the information in the window is correct and select **Submit**.

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

Virtual Sensor Installation

This section provides information about installing the ExtremeAnalytics Virtual Sensor.

You can install Virtual Sensor with one of the following methods:

- **ExtremeCloud IQ - Site Engine**: For more information, see ExtremeAnalytics Virtual Sensor Configuration in *ExtremeAnalytics User Guide*
- **vSphere Web client**: For more information, see Virtual Sensor Installation using vSphere Web Client on page 14

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

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 FQDN (`extremecontrol@<domain-name>`) for ExtremeCloud IQ - Sight Engine. `<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.

Prerequisites

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

- **ExtremeCloud IQ - Site Engine 10.04.10**: Configure SNMP and CLI credentials for Virtual Sensor in ExtremeCloud IQ - Site Engine. You must use SNMPv3 and the CLI credentials, and cannot have a blank password. For more information, see the Profiles section in *ExtremeAnalytics User Guide*.

- **Hypervisor**: 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 5: vCenter Global Permissions

| Privilege name	Permissions
Distributed Switch ◦ VSPAN operation	All
Datastore ◦ Allocate space ◦ Browse datastore	All

Host
◦ Local operations
  ▪ Create virtual machine
  ▪ Delete virtual machine
  ▪ Reconfigurevirtual machine
	All

Network ◦ Assign network	All
vAPP ◦ Import ◦ View OVF environment	All
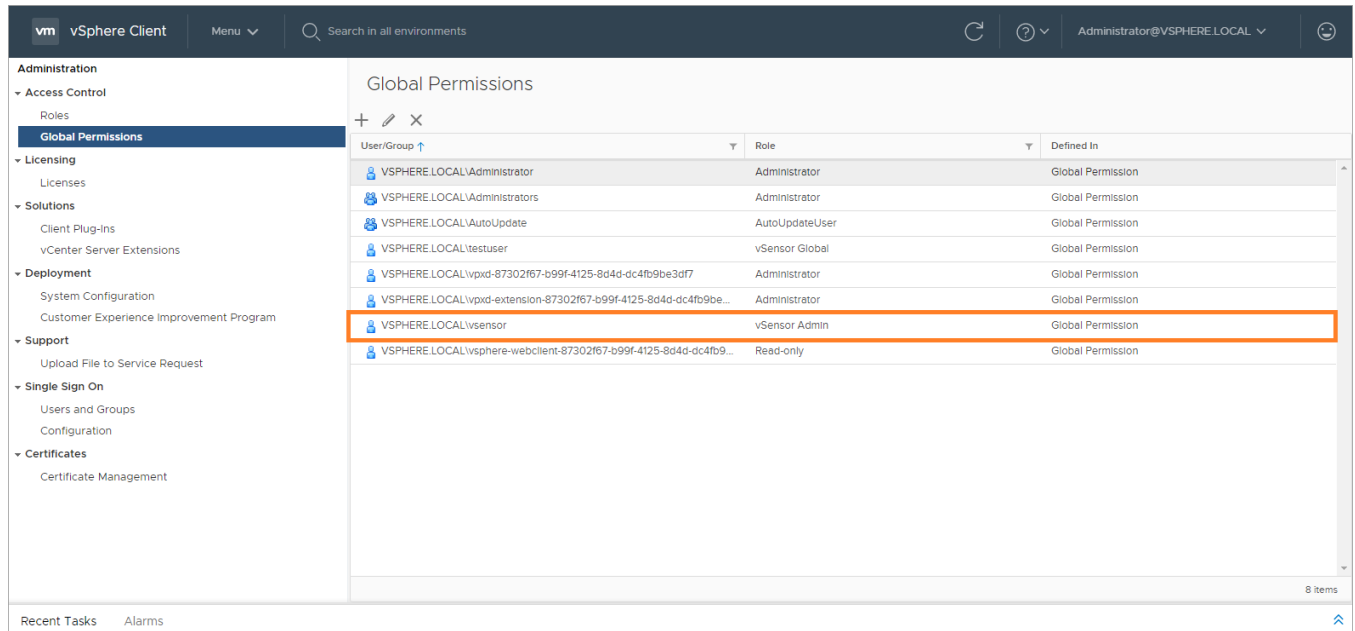
Configure vCenter vSphere login with an administrative role with the following permissions in the cluster the Virtual Sensor is monitoring:

Table 6: vCenter Global Permissions

Privilege name	Permissions
Distributed Switch ◦ VSPAN operation	All
Datastore ◦ Allocate space ◦ Browse datastore ◦ Remove file	All

Host
◦ Local operations
  ▪ Create virtual machine
  ▪ Delete virtual machine
  ▪ Reconfigurevirtual machine
	All

Network ◦ Assign network	All
Tasks ◦ Create task ◦ Update task	All

Table 6: vCenter Global Permissions (continued)

Privilege name	Permissions
vAPP ◦ Import ◦ View OVF environment	All

Virtual machine
◦ Change Configuration
  ▪ Add new disk
  ▪ Advanced configuration
◦ Edit Inventory
  ▪ Create new
  ▪ Remove
◦ Interaction
  ▪ Power off
  ▪ Power on
	All
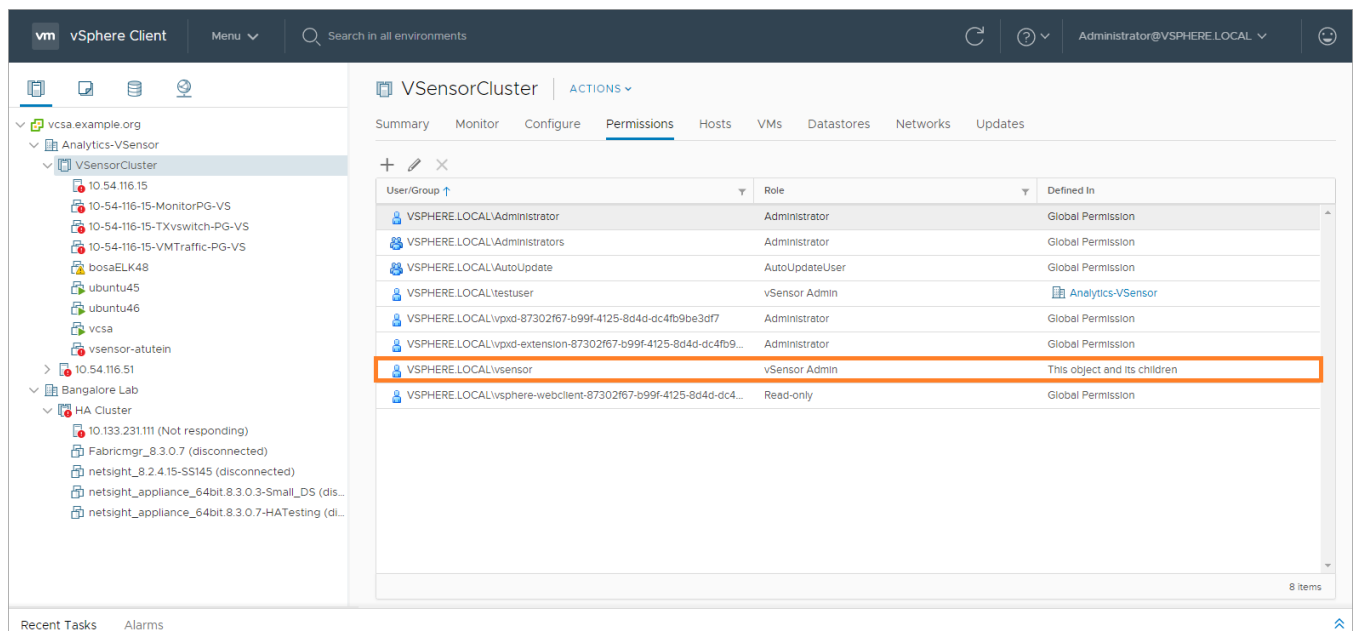
- **DHCP and DNS servers (required for ZTP+)**: Configure the DHCP and DNS servers on your network for discovery of the new Virtual Sensor deployment.

  For Virtual Sensor to communicate with ExtremeCloud IQ - Site Engine:
  - 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 ExtremeCloud IQ - Site Engine 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 ExtremeCloud IQ - Site Engine

Virtual Sensor can be installed using ExtremeCloud IQ - Site Engine. As a best practice, install
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 ExtremeCloud IQ - Site Engine,
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 ExtremeCloud IQ - Site Engine, 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 following image shows a typical Virtual Sensor deployment on a VMware ESXi hypervisor.
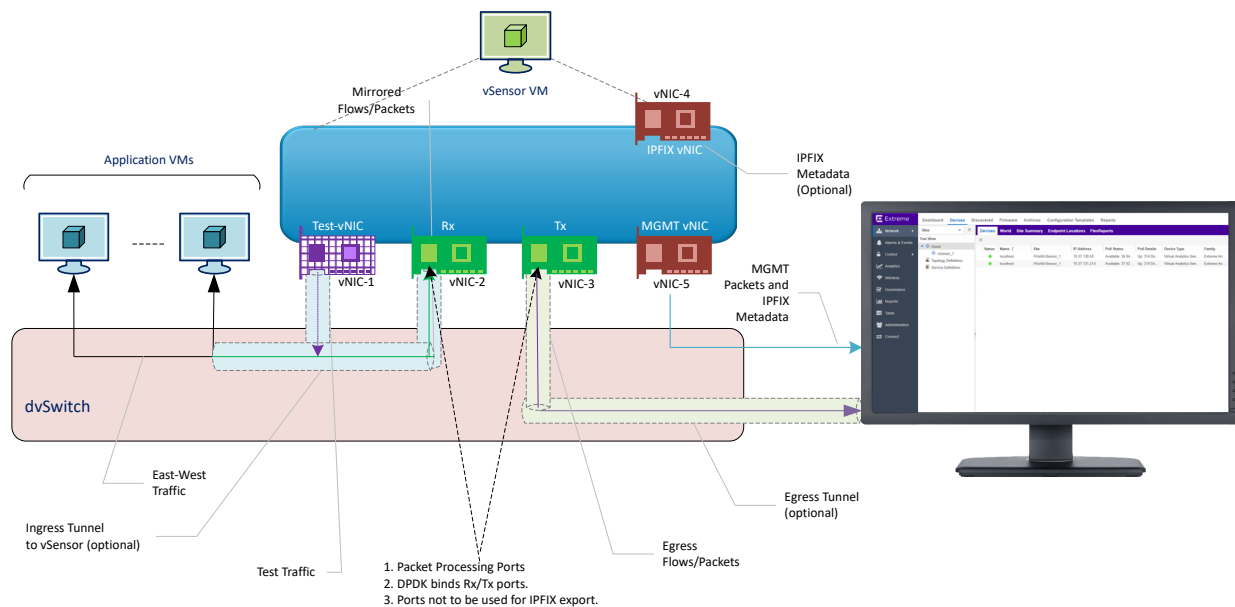
Figure 1: Deployment architecture

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 ExtremeCloud IQ - Site Engine 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 ExtemeAnalytics 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.

Install 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 device 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 user name and password, and select **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**.
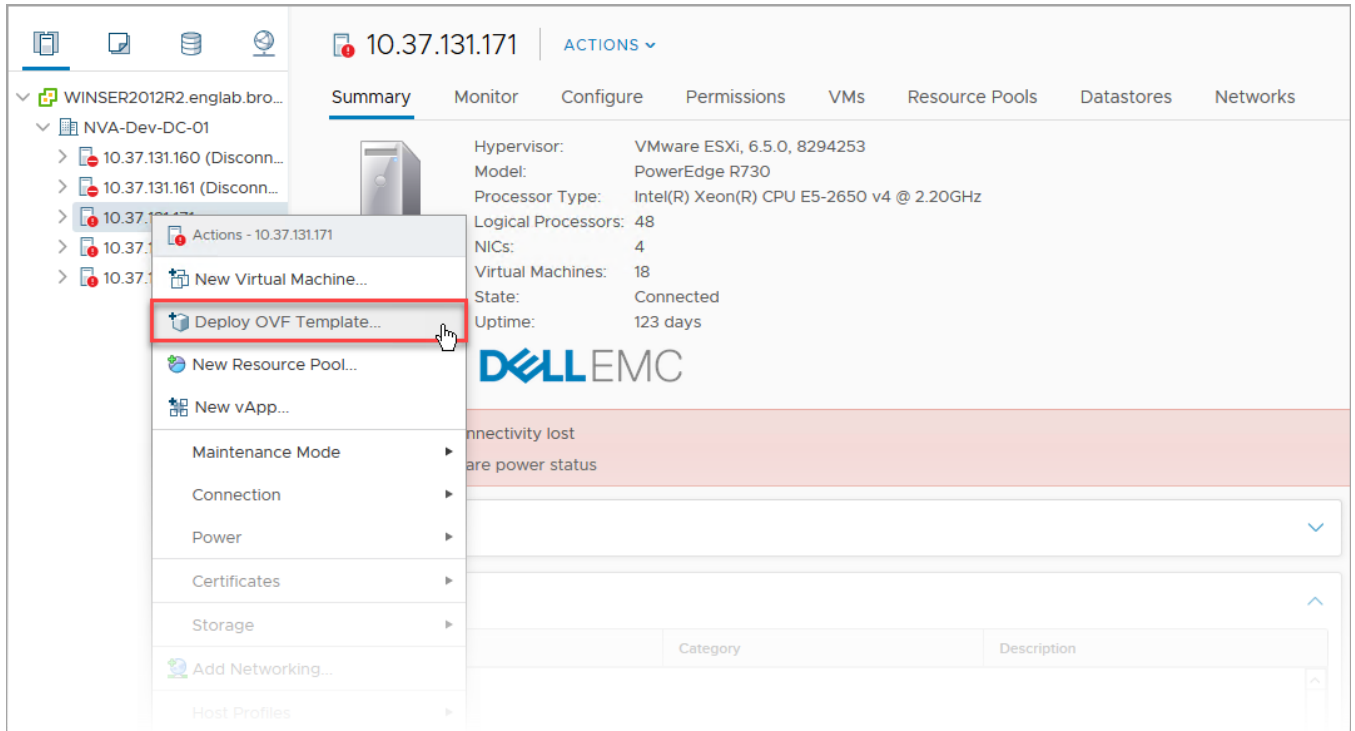

Figure 2: Deploy OVF Template

Deploy OVF Template window appears.

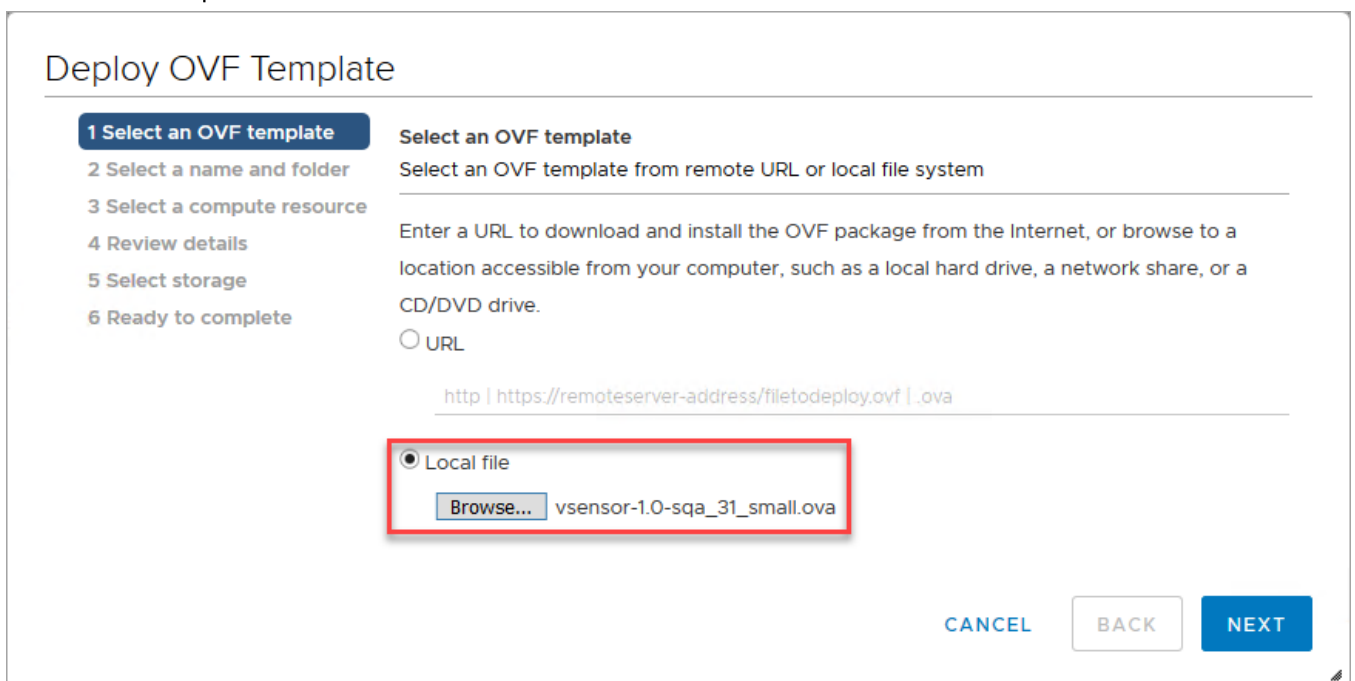   b. Select **Browse** to select the Virtual Sensor OVA image you downloaded in 1 on page 16 and click **Open**.

Figure 3: OVA image

     c. Enter a name and the location for your virtual machine.

     d. Select the destination compute resource.

     e. Review the details for the selections and select **Next**.

     f. Select **Next**.

       The **Select storage** page opens.

     g. Select a datastore from the list of accessible datastores and select **Next**.

       The **Select networks** page opens.

     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 ExtremeCloud IQ - Site Engine and Analytics engine.

         • **TestIntfNetwork** and **IngressNetwork** must be on a port group on the dvSwitch you want to monitor.

Figure 4: Select networks

Table 9: 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.   Select **Next**.

       The **Customize template** page opens.

Enter appropriate values for the following properties:

Table 10: 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	Host name for the VM. The length of the host name can be up to 64 characters. It can contain alphanumeric characters and hyphens. **Note:** Host name cannot start or end with a hyphen.
Domain Name	
DNS IP Address	This is the DNS server IP address. This is mandatory.
NTP IP Address	NTP server IP address.
NTP Timezone	Network Time Protocol (NTP) time zone. For example, `America/New_York`. Run the following Linux command to list the available time zones: ` timedatectl list-timezones`
ExtremeCloud IQ - Site Engine IP Address	(Optional) If this IP address is not provided, it is assigned by the DHCP server.
Root password	This is the password for the root user on the ESXi host on which Virtual Sensor is being deployed. **Note:** If CLI credentials for Virtual Sensor are already configured in ExtremeCloud IQ - Site Engine, those credentials take precedence over the password set here. For information, see the"CLI Credentials" section in *ExtremeAnalytics User Guide*.

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 beginnng 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

Figure 5: Customize template

j. Select **Next**.

The **Ready to complete** page opens.

k. On the **Ready to complete** page, review the configuration settings for the virtual machine.

l. Select **Finish**.

The virtual machine is displayed 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 provided the ExtremeCloud IQ - Site Engine IP address, Virtual Sensor tries to connect to ExtremeCloud IQ - Site Engine 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 for installing Virtual Sensor on more ESXi hosts.

Complete the remaining steps in ExtremeCloud IQ - Site Engine 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

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 11:

Option	Description
Reservation	Reservation = number of vCPUs * CPU speed of ESXi **Example** • Medium OVA: 2 * 2297 = 4594 MHz • Small OVA: 1 * 2297 = 2297 MHz
Shares	Set this to **High**.

4. Select **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. Select **Yes** to continue with the upgrade.
7. Power on the virtual machine.

Creating a Port Mirroring session to monitor traffic

Perform the following steps to create a port mirroring session:

1. Log in to the vSphere Client and:

    a. Select the **Networking** tab.

    b. Select the Distributed Switch you want to configure.

        `vsDSwitch1` is used in this example.

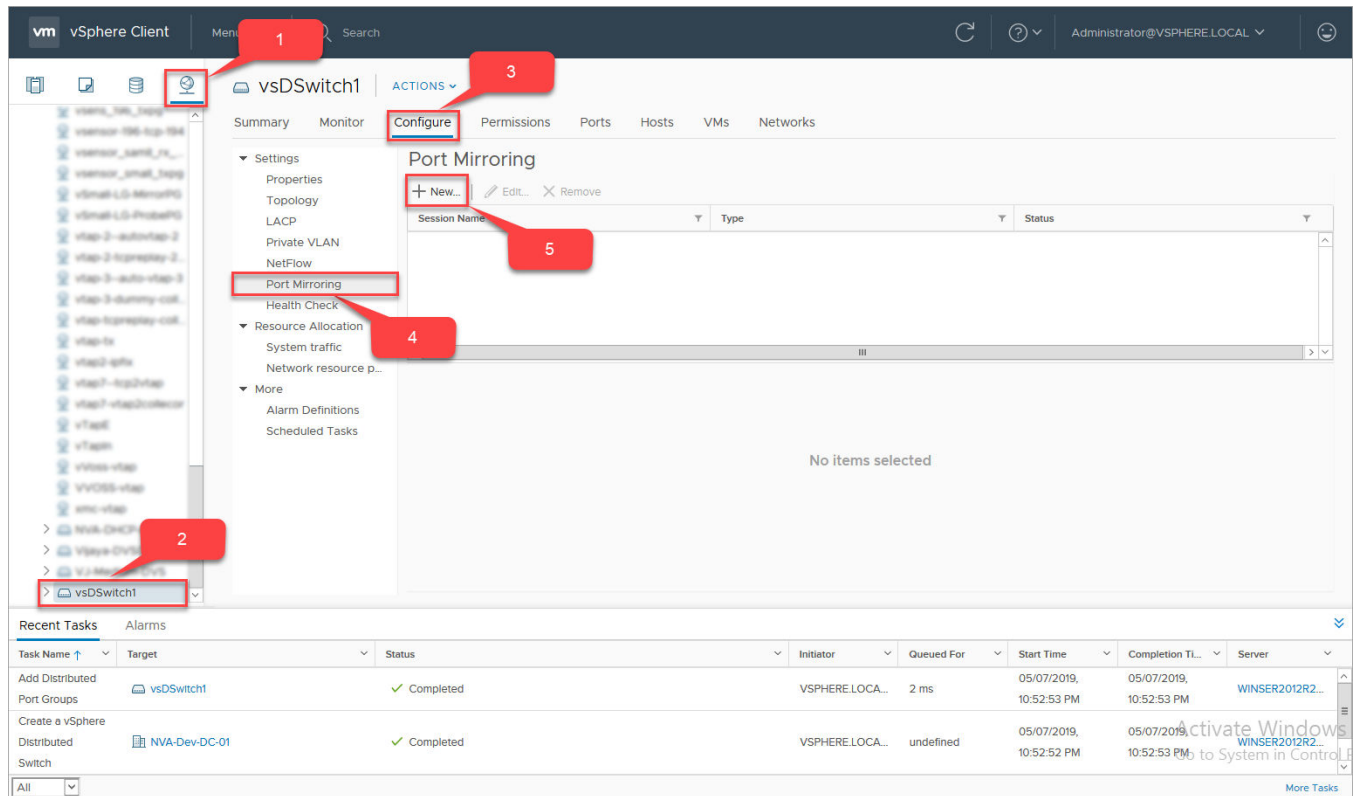   c. On the **Configure** tab, select **Port Mirroring**.

Figure 6: Port Mirroring

2. Select **New**.

   Add Port Mirroring Session window opens.

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

Figure 7: Add Port Mirroring Session

   Select **Next**.

3. In the **Edit properties** section:

   - Enter a meaningful name in the **Name** field
   - Change **Status** to **Enabled**.

   All the other fields remain unchanged.

Figure 8: Edit properties

Click **Next**.

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

   Select Ports window opens.

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

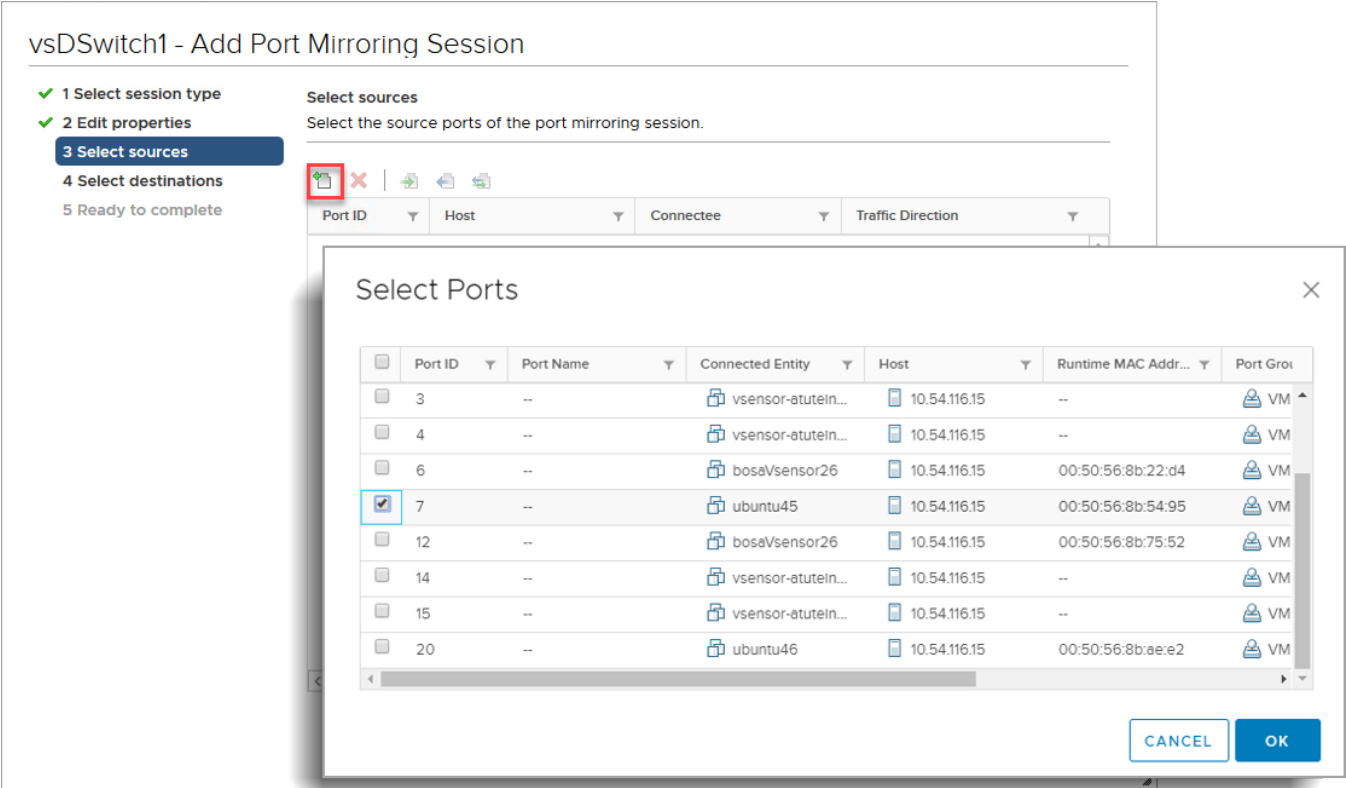   Optionally, change the mirror to either Ingress or Egress, or leave it as Ingress/Egress.

Figure 9: Select Ports

The selected ports appear in the list.

Figure 10: Select source ports

Select **Next**.

5. In the **Select destinations** section, select 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.
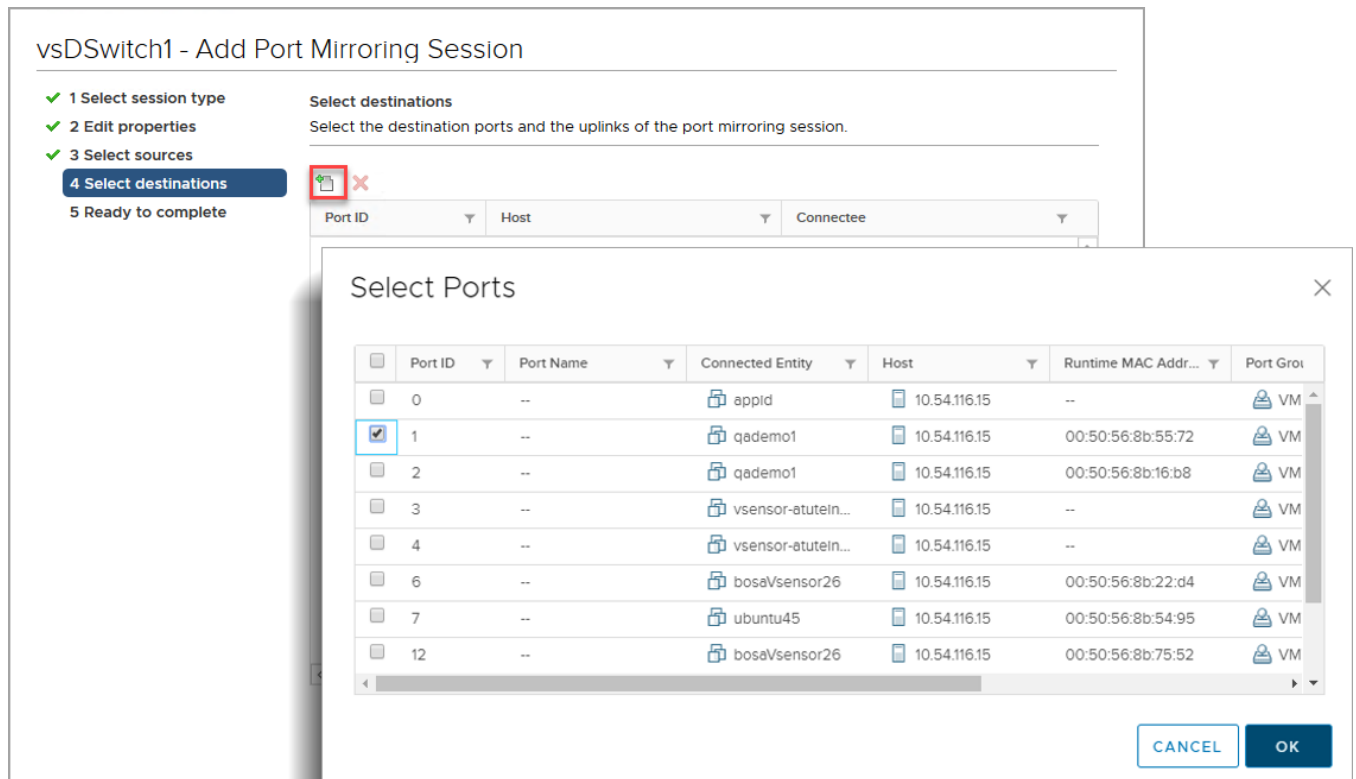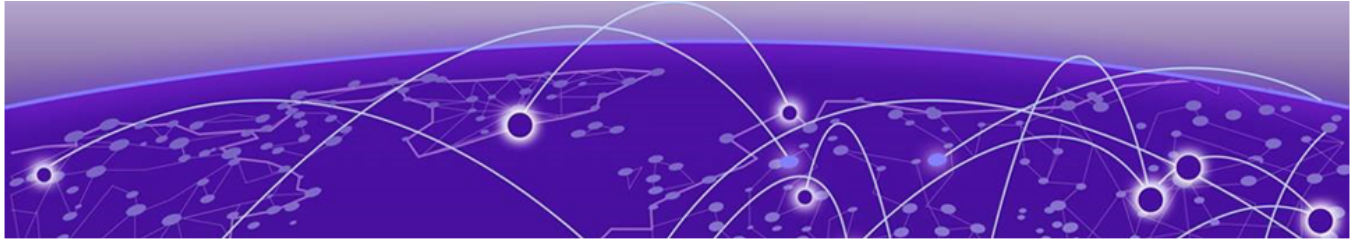

Figure 11: Select destination ports

6. Select **Finish**.

Post-installation Configuration

This topic provides information about the steps to be performed in ExtremeCloud IQ - Site Engine to discover and display the device.

1. Log in to ExtremeCloud IQ - Site Engine 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.
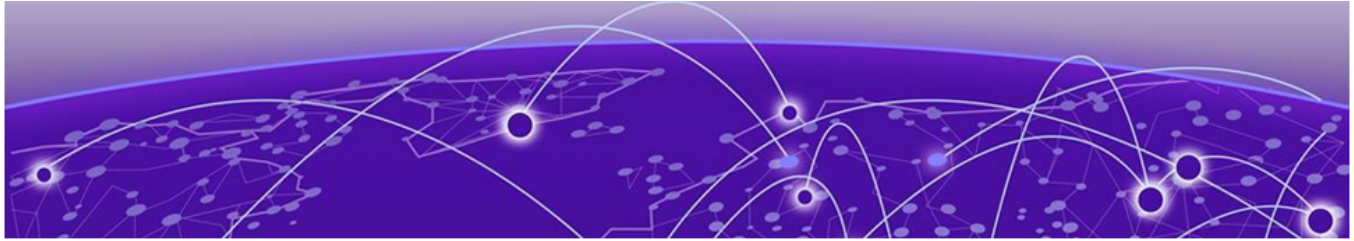
Troubleshooting

This topic 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. Log in 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:
   - **ExtremeCloud IQ - Site Engine**: 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 14