tripwire®

TRIPWIRE®
INDUSTRIAL
VISIBILITY

TRIPWIRE INDUSTRIAL VISIBILITY 4.2.4
QUICK INSTALLATION GUIDE

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Quick Installation Guide Revisions

Rev	Date	Owner	Author	Revisions
Rev 1	April 2021	Moshe Alvoer	Beth Stolper	Initial Version

Contents

1 Introduction

This document provides the quick installation procedure for Tripwire Industrial Visibility (TIV), version 4.2.4 and above.

> **Note** TIV supports RHEL/CentOS up to version 7.9 minimal.

2 Network Preparation TIV Installation

The TIV has 3 different options for collecting data from your system. The main setup is a passive monitoring on a SPAN/Mirror port on a central switch. All traffic routed to the SPAN port will be analyzed and presented in the TIV user interface. To be able to get more details on each asset, you can use the AppDB option or the Active Query option.

If you have traffic in your system that does not pass the SPAN port, i.e. a local RTU on a remote location, then you can use a sensor installation. The sensor will operate similar to TIV setting up a baseline and alerting if you have deviations from the baseline. The data is compressed and encrypted and sent to the central TIV.

To be able to see all assets in your system, you need to evaluate the topology to find the most propriate placement, and then reconfigure some of the switches to span the traffic to the point where the TIV is placed.

2.1 Network Setup Procedure

1. Decide which assets you want to monitor. Typically, you will take your topology drawings of the control system and mark the systems you want to include. If possible, set up a list of all assets you expect to see. Then you will be able to evaluate the hit-rate of the asset discovery in TIV.
2. The best placement is often close to the SCADA and Engineering stations. This is centralized positions where data from a lot of assets are passing by. Choose a switch in this position.
3. Analyze the traffic flow in your system. If the system is segmented with a VLAN structure, you can SPAN one or more VLANs to the selected SPAN port.
   BE CAREFUL! Check the load of the switch and evaluate the amount of data before you do the SPAN.
4. You can also SPAN physical ports on the switch, like the ports connected to the SCADA server, Engineering stations, historian servers and asset management systems.
5. After TIV has been running in learning mode for a while, you can start to enrich the assets data by importing the PLC/RTU program files by using the AppDB import. This will give you a more detailed picture of the assets with vulnerabilities, and it will also show the nested devices in the back of a PLC.
6. Next step will be to do dedicated active queries to assets like servers. This will give you more detailed information about programs installed, patches and versions. A more detailed list of vulnerabilities will show up.

7. Compare your asset list with the discovered assets in TIV. If some assets are missing, check the communication paths. Maybe you need to install a sensor or SPAN more VLANs/ports into the TIV monitoring port.

3 ClarotyOS Wizard [Only Admins]

3.1 Quick Installation via ClarotyOS

- Insert the installation file to your server.
  - Either install directly with ClarotyOS's ISO or with a bootable media file containing the ISO.
- Open the Server Console and select Install ClarotyOS:

Figure 1 Installing ClarotyOS

- Wait until the installation is finished; the following screen appears:

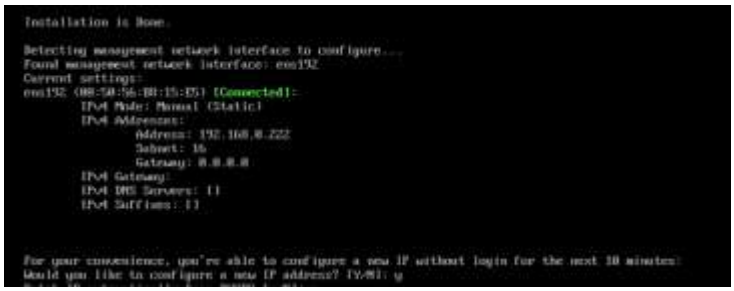


Figure 2 ClarotyOS installation complete

- Note that in the first installation, you can opt to change the IP address once.
- You can reconfigure your network settings by entering the Admin password and then **Run**.
  - Wait until the machine IP is presented.
- Choose whether you prefer to configure your IP via a console using CLI or via the TIV UI; then continue to the TIV Wizard.

3.2 Deploying via OVA

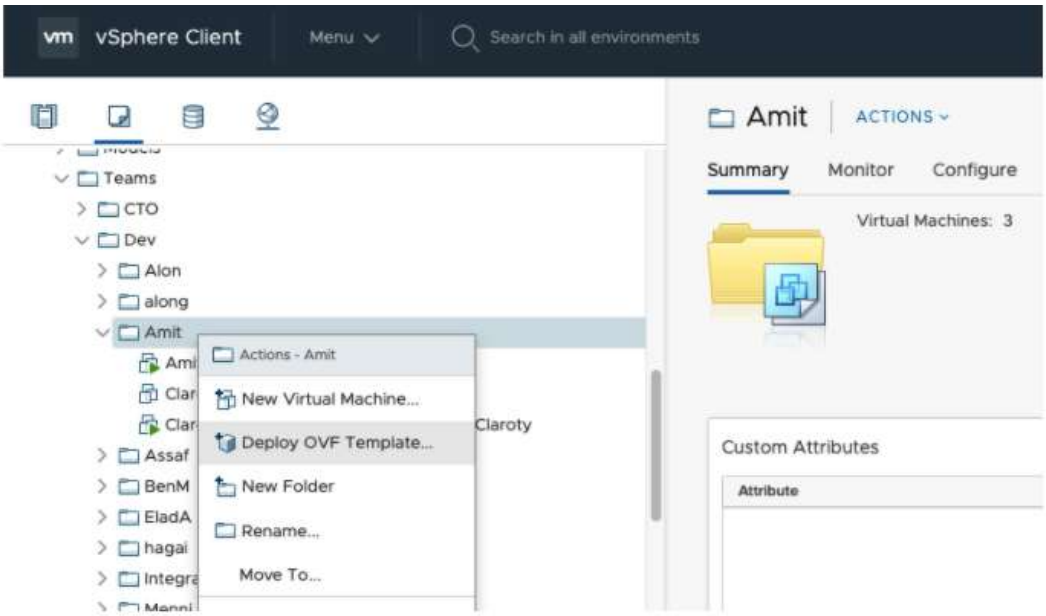
In order to deploy ClarotyOS as a ready-to-go VM, make sure you have:

1. The .ova file of ClarotyOS
2. Optional: An settings.iso file with your deployment settings. This file will be generated by the Tripwire team.

3.2.1 Deployment on VMware vCenter

- Log into your vCenter UI, and go to the folder you want to deploy the VM in.

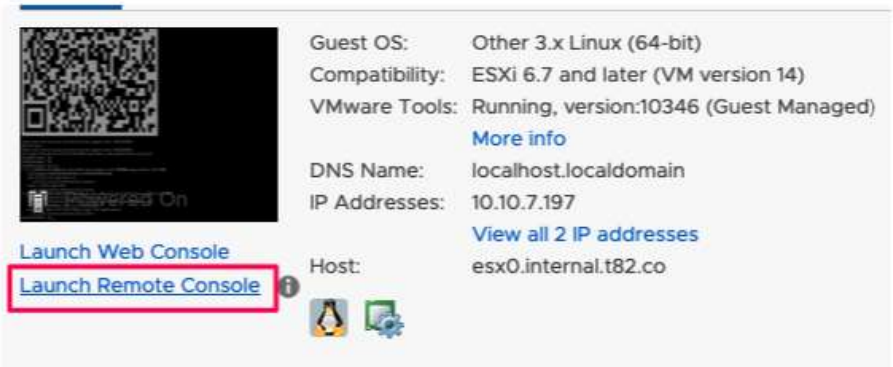
  Right-click on the folder and select “Deploy OVF Template”



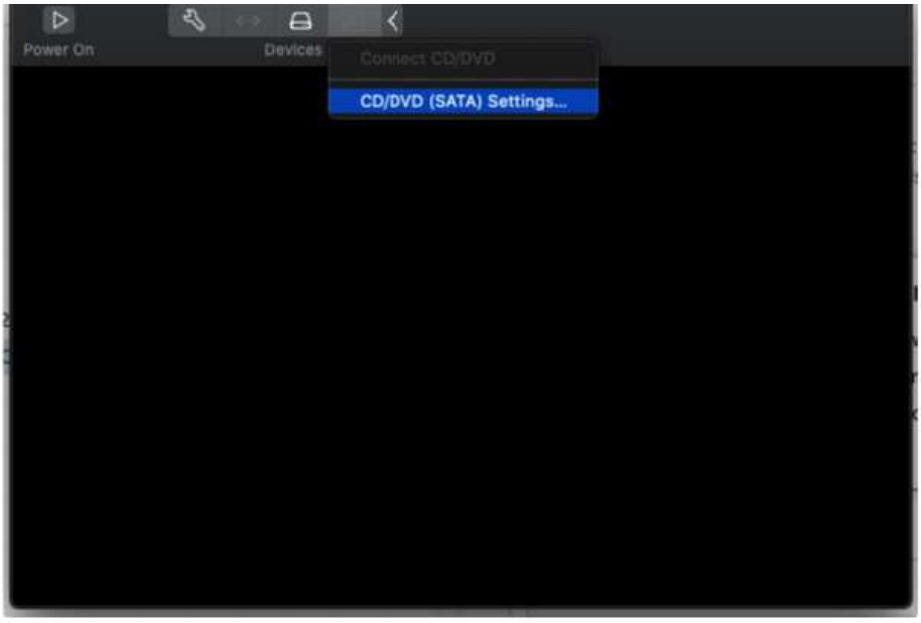
- Select the OVA file and click Next:

- Continue the wizard and select the name of the VM, the folder, the ESX, and the storage.

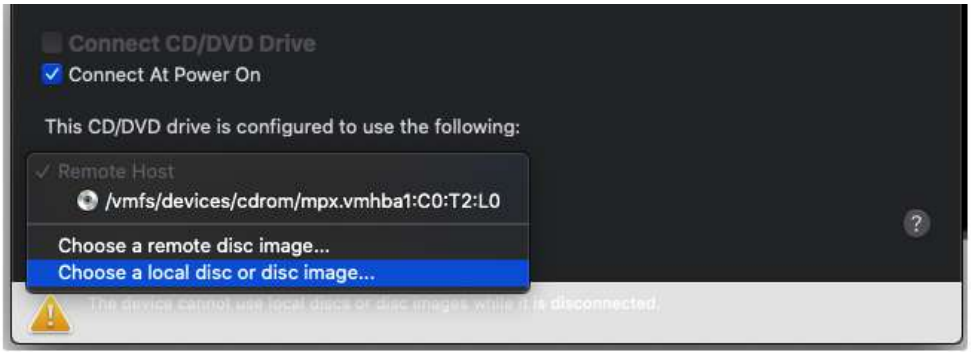
- When the wizard is done, you will have the machine powered off in your folder. DON'T TURN ON THE MACHINE YET!
- Right-click on the machine, choose "edit settings", and configure the VM CPU and Memory allocation to your needs. You may also increase the size of the Hard Disk, but you will have to do a manual command later in the admin shell in order to make the VM see the change admin@localhost# storage extend-device.
- If you don't have a settings file, you may turn on the machine and configure it through the ClarotyOS Wizard.
- If you have a settings.iso file, before turning the machine on, open the machine console through "Remote Console". You may get the installation of "VMware remote console" from their website if you need it.



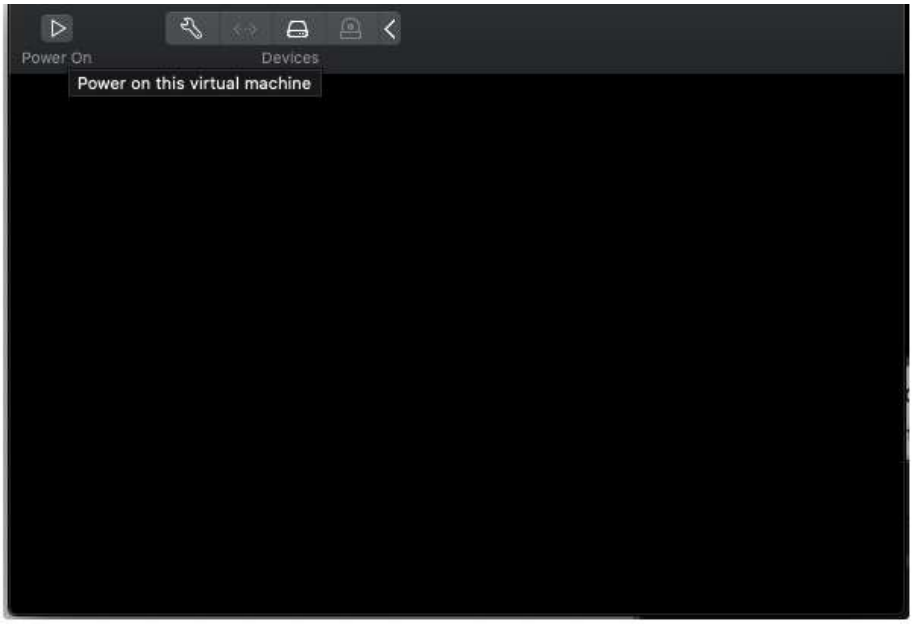
- On Vmware Remote Console, click the disc icon and select "CD/DVD Settings"



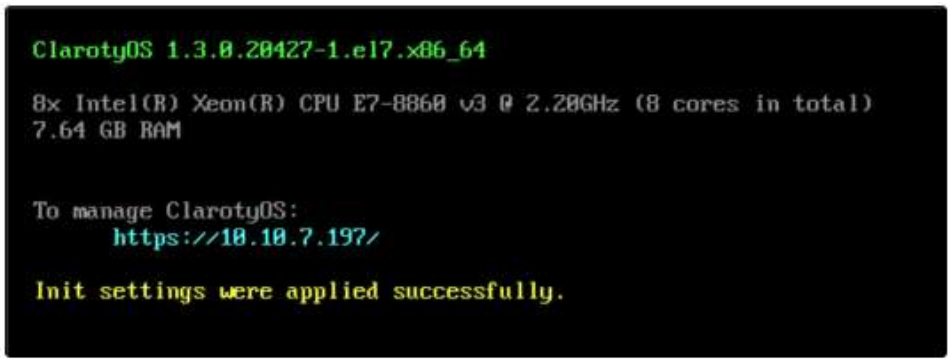
- Check the "Connect At Power On" checkbox. Then click on "Choose a local disc or disc image" and choose the provided "settings.iso" file. After, you can close this window.



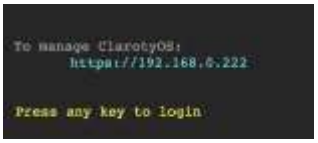
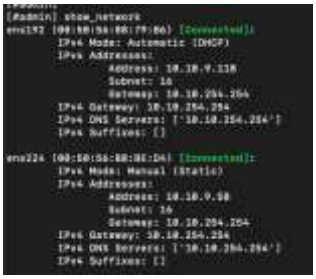
- Now, turn on the machine using the "Power On" button on the top of the screen:



- A minute or two after the machine will finish the boot, it will read the settings from the iso file and apply them. Once the process is done, you will see a message is the machine console:



3.3 Configuring your IP via a Console using CLI

1.	Open your server's console and press any key	
2.	Connect with Admin User	
	Default password: ■ "Password1!"	
	■ Change the Default password	
3.	Change your IP Address:	
	a. Use "show network" to see your current configuration	
	b. Use "network interface configure <interface-name>" to Change IP Address, Subnet, Gateway, DNS, and suffix or choose to get IP from your DHCP.	
4.	Open a browser session	
5.	Go to https://<Your New IP Address>/	
6.	Continue to the TIV Wizard	

3.4 Configuring your IP via the TIV UI

- Wait until the machine IP is presented.
- Go to https://192.168.0.222/; this is TIV's default IP.
  - Ensure that you are in the same network and subnet (192.168.0.0/24)
- If you cannot connect in this manner, follow the CLI instructions.
- Continue to the TIV Wizard.

3.5 Configuring your Network Settings

- Enter the IP address of the machine in the Web Browser.
- Read and confirm the End User License Agreement (EULA).
- Configure your server's network.

> Alternatively, you can get the IP from automatically from your DHCP.

Figure 3 Network Configuration Example

- Configure your server's time. You can set your time by NTP server or sync with your local time:

Figure 4 Configuring the Server Time

- Press **Next**.
- Make sure your network settings are defined correctly before committing them:

Figure 5 Setting the Configuration

- Press Set Configuration.
  - During the configuration process the following screen appears:

Figure 6 New Configuration set up

- The system redirects you to the TIV Wizard.

4 TIV Wizard [Only Admins]

4.1 Choose the Product Type

Choose which TIV product to install:

Figure 7 Product Type selection

- If you choose to install an **EMC** or a **TIV Site,** the additional configuration options are as follows:

Figure 8 Configuring Additional Options for TIV Site

- **Active Query** – When selected, TIV's Active Query data collection enables active discovery of assets by scanning and then performing precise queries tailored to the network typography. Active Query is disabled by default. For more information refer to the *TIV User Manual: Active Queries.*
- **App DB** – When selected, TIV's Application Database (App DB) mechanism onboards assets from PLC configuration files or projects to

enhance asset coverage. It is enabled by default as shown above. App DB extends the system's asset inventory by including assets that are not available directly through the network. For more information refer to the *TIV User Manual: AppDB.*

- **Cloud** – When checked, Cloud updates are configured as described in the *TIV Reference Guide*.

- As described above, choose to activate Active Query, App DB and/or Cloud detection, and press **Next**.

4.2 Activate the License

You can start with the production license or opt to use a temporary license for the initial 14 days.

Contact Tripwire to get a TIV **License Key**.

- Approve the **License Agreement** and set the TIV network configuration.
- Wait until the **License Activation** screen shows up.
- Obtain a License Key from Tripwire (as described below) using the UUID that you see on the screen, enter it into the system and press **Activate**; or click the **Skip** option to use a temporary license (which is valid for 14 days).

Figure 9 License Activation screen

- To apply for the license for your production server, please contact https://license.claroty.com/login

  with your Salesforce user and generate a new license with your UUID from the token that has been assigned to you.

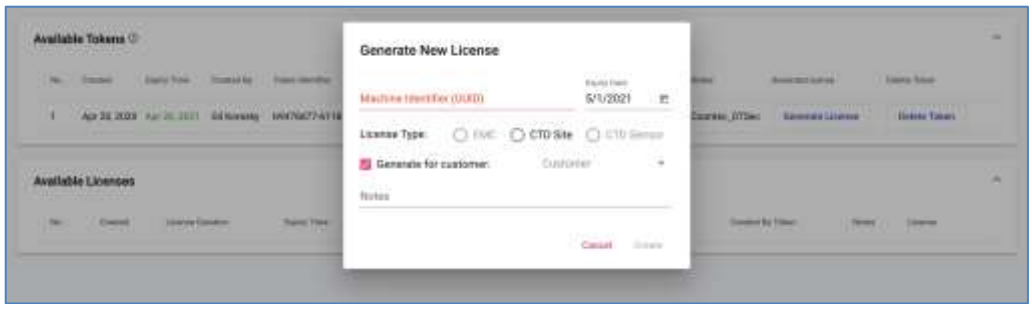


Figure 10 Generate a New License screen

- After successful installation, you can access the license info via the **Configuration > License** page. The license info screen will display the license, UUID and expiration details as shown in the example below:

Figure 11 License Info

> Note If you cannot connect to the Tripwire portal, please contact Tripwire Support.

4.3 Site Information

The EMC is TIV's central appliance, usually located at the Security Operations Center (SOC) or at the corporate site, and you can name it as you wish.

Enter an appropriate name and an optional description for the machine you are configuring and then press **Next**.

Figure 12 Site Info for an EMC

Figure 13 Site Info for a TIV Site

4.4 Change Password (for EMC or TIV Site)

In order to increase security, you can change your default password:

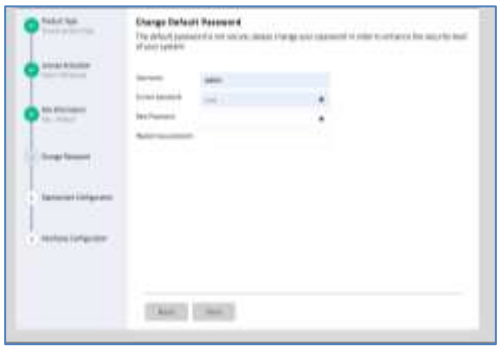


Figure 14 Change Default Password

This is the last step for the EMC setup.

4.5 Deployment Configuration

The next step is to set the Deployment Configuration, which differs for each product type.

4.5.1 TIV Site: Site Information and Deployment Configuration

The TIV Server performs DPI processing and will process the data from desired network.

Figure 15 EMC Information for connecting to TIV Site

- To connect the TIV Site to the EMC, enter the EMC IP address and the **Access Key** or choose **Skip** if the EMC is not configured.
  - **EMC Access Key** – The access key is a password from the EMC. It lets the TIV Site authenticate with the EMC or the Sensor authenticate with TIV Site. The EMC's access key is accessible in **Configuration > Management > Deployment Architecture > Deployment Configuration**:

Figure 16 EMC Access Key

4.5.1.1 Interface Connectivity for TIV

1. Select to process data to the desired interface from which the system will collect data:

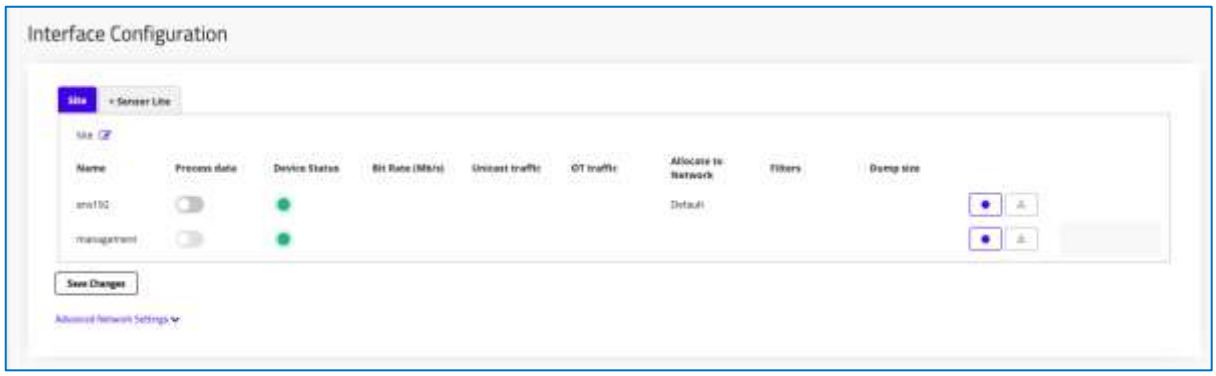


Figure 17 Interfaces Configuration

1. **Process Data** – Button for obtaining more information about the interface. OFF by default.
2. **Device Status** – If the interface link is UP (connected) it is a Green dot; if it is DOWN (disconnected or unavailable) it is a Red dot.
   a. **Bit rate** (MB/s) – Describes the amount of traffic passing in this interface
   b. **Unicast Traffic** – Describes the quality of your traffic by counting unicast packets (Low, Medium, High)
   c. **OT Traffic** - Describes the amount of OT traffic on this interface (Low, Medium, High)
3. **Allocate to Network** – Displays the Network this interface is connected to. You can add new network. Each interface can be connected to one network.
4. **Filters** – Use this button to add filters to the traffic in the network, such as tcpdump capture filters.
5. **Record** – Press this button when you want to record a PCAP file for the traffic on a network for investigating the PCAP file.
6. **Download** – Press this button to download the recorded PCAP file to your machine
7. **Dump Size** – Shows the size of the network traffic file that was recorded.
8. **Save Changes** – Press when done to commit your settings.

4.5.1.2 Advanced Network Settings

Open this area to configure the following advanced network settings:

1. **Network** – Set to Default. Use the Edit button to modify your network settings.
2. **Store Raw Data (PCAP)** – When selected, this button lets you to save a .pcap file for each alert that raised in the system.

3. **Known Threat Alert detection**– TIV uses a sophisticated signatures-based database in order to identify known attacks. We recommend setting this button to ON.

You have successfully finished installing the system.

Refer to the *TIV User Guide: Interface Configuration* and *Configuring Log Settings* for configuration details.

4.5.2 TIV Sensor: Deployment Configuration

Set the details for your TIV Sensor as follows:

Figure 18 TIV Sensor Configuration

- Enter the Sensor **Name*** (mandatory)
- Provide an informative **Description** (optional)
- Set the **Site address** and **Access key**:
  - **Access Key for the Sensor** – The access key for the Sensor is a password from the Site. It lets the Sensor authenticate with TIV Site. You can find the access key in **Configuration > Management> Deployment Configuration > Deployment Architecture**.

You have successfully finished installing the TIV Sensor.

Figure 19 Sensor setup complete

4.5.2.1 TIV Sensor Info in TIV

Enter the TIV Site UI, and navigate to **Configuration > Management > Deployment Architecture > Deployment Configuration**:

Figure 20 Sensor Info screen in Configuration > Management > Deployment Architecture > Deployment Configuration

The Sensor tab will now appear in the Interface Configuration page with the relevant properties:

Figure 21 Sensor Tab in Configuration > Data Sources > Interface Configuration

4.5.3 TIV Sensor Lite: Deployment Configuration

The TIV Sensor is designed for setups in which the bandwidth between the TIV Sensor and the TIV Server is very limited and should be limited to a bare minimum. It will connect to the TIV site and send data.

4.5.3.1 Interface Connectivity for TIV Sensor Lite

From TIV, connect to the Sensor as follows.

1. Navigate to Configuration > Data Sources > Interface Configuration.

Figure 22 Interfaces Connectivity

2. Select the **Sensor Lite** tab and enter the following information:

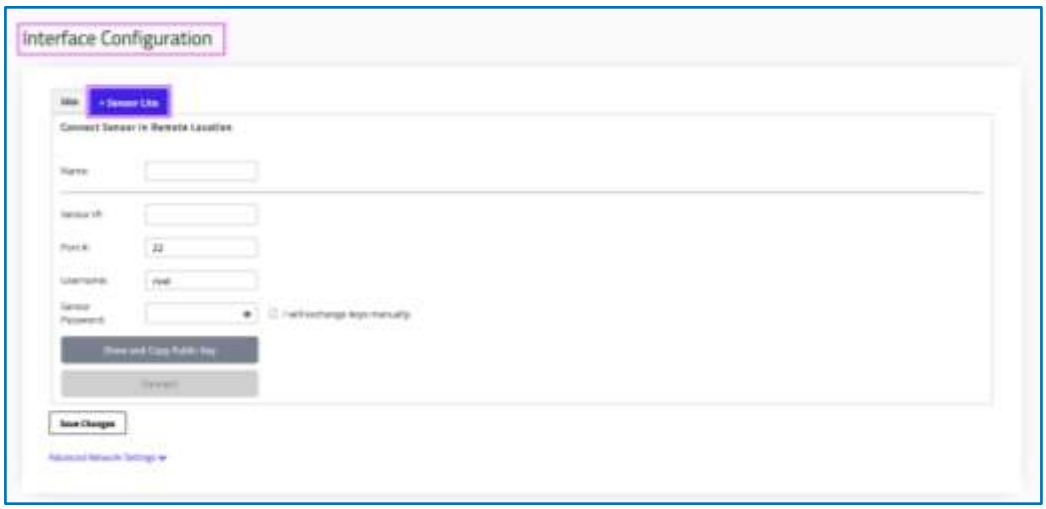


Figure 23 Sensor Lite tab

a. **Name** – The name of the sensor

b. **Sensor IP** – The IP address of the sensor

c. **Port#** – Enter the desired port. The default port is 22

d. **Username** – Enter the username for the sensor

e. **Sensor Password** – The sensor's password

f. **Save Changes** – When all the information is correct, press **Save Changes**.

For **Advanced Network Settings**, see section 4.5.1.2 above for modifying the network, storing raw data and using Known Threat alerts for the sensor.

You have successfully finished installing the sensor. The Sensor Lite tab now appears in the Interface Configuration page with the relevant properties:

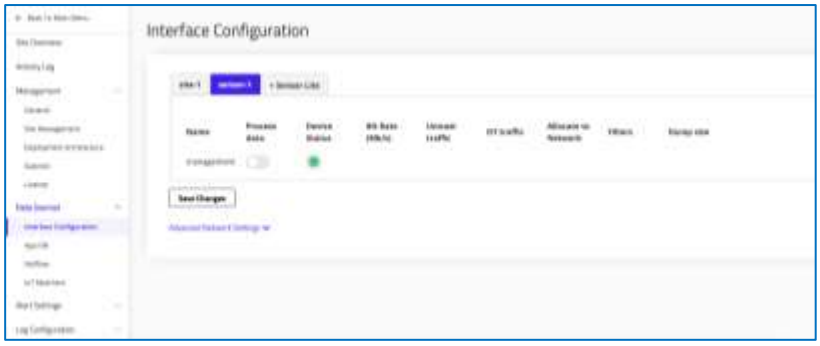


Figure 3 Sensor Lite Tab in Configuration >Data Sources > Interface Configuration

5 Upgrades

Prerequisite: First, upgrade the EMC with the following instructions. After the EMC finishes upgrading, you can upgrade the connected sites automatically through the EMC.

To upgrade the EMC/TIV manually:

- Go to the **ClarotyOS Configuration** page (through TIV) and navigate to the **Upgrade** tab.
- In the Upload Bundle area, upload your upgrade bundle and click Upload File.

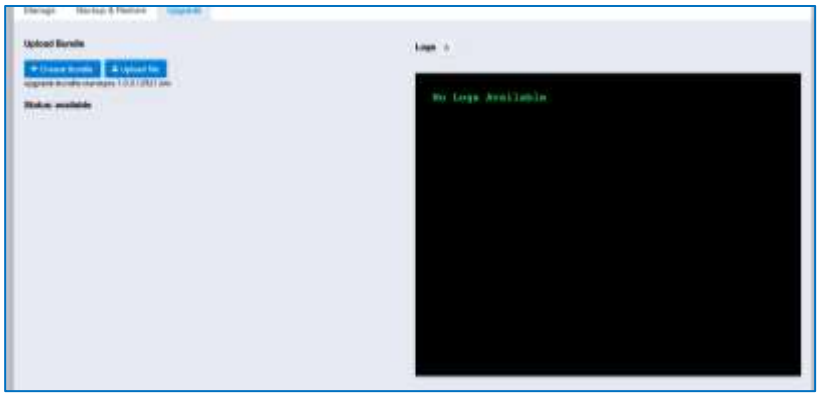


Figure 25 Upload the bundle

- Wait until upload is finished.
  - Follow the green progress bar on top

Upgrade your machine from by clicking on the Upgrade tab:

- **Choose Bundle** – Choose a file from TIV in order to get specific fixes or upgrades
- **Upload File** – Upload to TIV in order to upgrade your machine to a higher version or to allow specific fixes.

> Note Watch the logs to ensure your upgrade was successful. If it failed, please consult Tripwire Support and send the presented logs.

- Read the Bundle Information and click **Upgrade**:

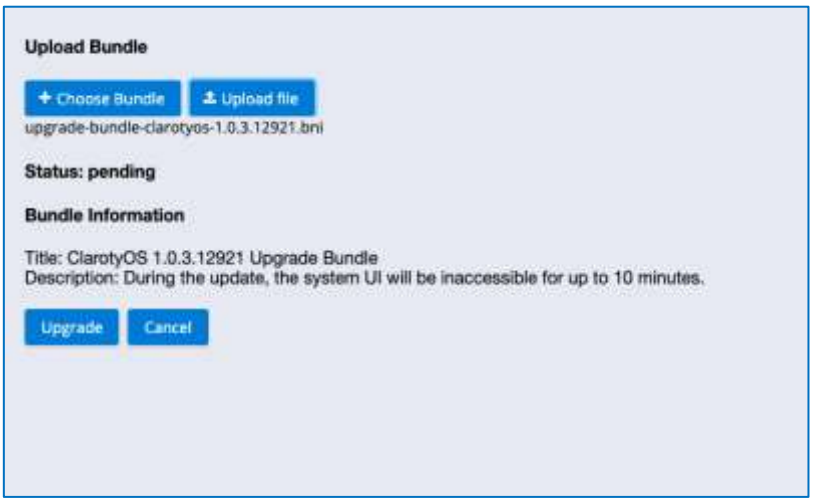


Figure 26 Bundle Information

- Wait
  - Follow the upgrade's logs on the right side of the screen:

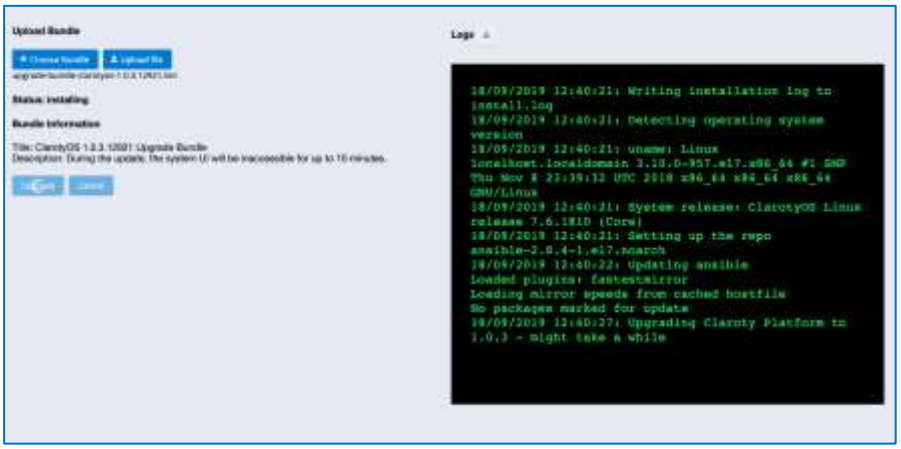


Figure 27 Read the Logs

> **Note** If the service will be restarted during the upgrade, your connection will be lost for a few minutes.

- When the upgrade is finished, the Status will change to "Success" or "Failed".

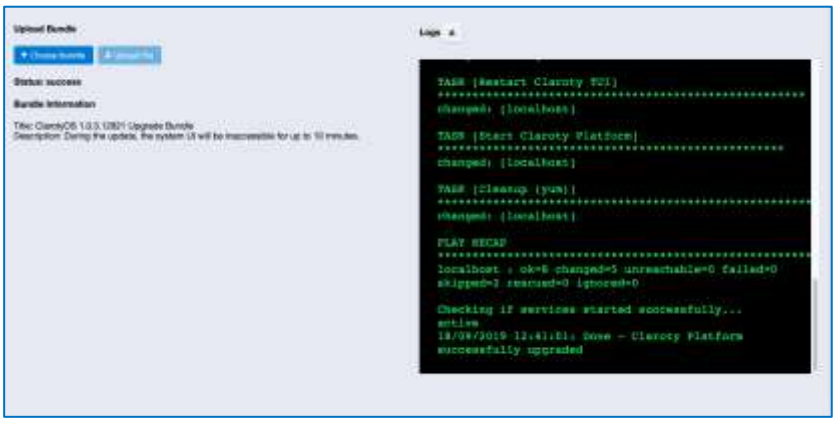


Figure 28 Upload bundle

- You can download the logs file (on the top-right download button).

After the EMC upgraded successfully, you can login to the site maintenance window and upgrade your connected TIV site.

> Note: The connected sensors will be upgraded by default after the TIV is upgraded.

Figure 29 Site Maintenance

6 Add a new hard disk or extend an existing one

This command allows you to add or expand hard drives in your ClarotyOS and add the extra space to the filesystem.

6.1 Option1: Adding a New HD

This command adds a new partition, creates PV, extends VG size, extends LV size, and resizes the XFS filesystem's size for you.

In order to add your new HD to the current filesystem, login to admin's shell and run:

```
storage add-device
```

- Choose wanted device from list:

- Approve:

- Approval message:

Creating partition, adding new "Physical Volume"

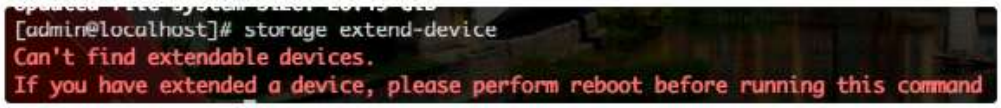
6.2 Option2: Extending an Exiting HD

This command resizes the partition size, resizes PV size, extends LV size, and resizes the XFS filesystem's size for you.

- In order to extend your HD and resize current filesystem size, login to admin's shell and run:

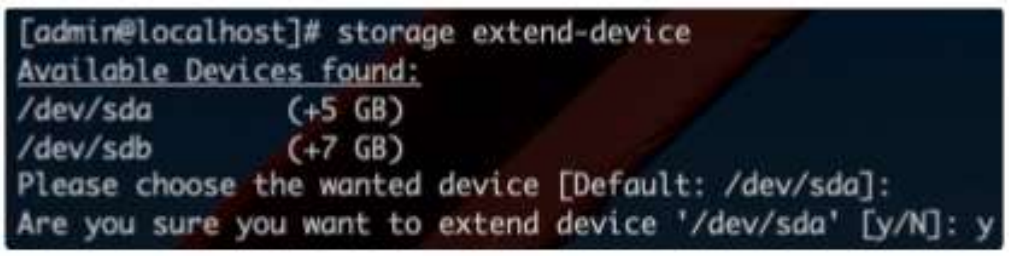
```
storage extend-device
```

> Note If you can't find the device you have extended in the list please perform a reboot and try this command again:



- Choose the wanted device from the list:

- Approve:



- Approval message